This document is subject to the provisions of the Privacy Act of 1974, and may require redaction before disclosure to third parties. No redaction has been performed by the Office of Inspector General. Recipients of this report should not disseminate or copy it without the Inspector General's approval.

REPORT OF INVESTIGATION

UNITED STATES SECURITIES AND EXCHANGE COMMISSION
OFFICE OF INSPECTOR GENERAL

Investigation Into Misuse of Resources and Violations of Information Technology Security Policies Within the Division of Trading and Markets

Case No. OIG-557

August 30, 2012

This document is subject to the provisions of the Privacy Act of 1974, and may require redaction before disclosure to third parties. No redaction has been performed by the Office of Inspector General. Recipients of this report should not disseminate or copy it without the Inspector General's approval.

REPORT OF INVESTIGATION

UNITED STATES SECURITIES AND EXCHANGE COMMISSION OFFICE OF INSPECTOR GENERAL

Investigation Into Misuse of Resources and Violations of Information Technology Security Policies Within the Division of Trading and Markets

Case No. OIG-557

Introduction and Summary of the Results of the Investigation

The Securities and Exchange Commission (SEC or Commission) Office of Inspector General (OIG) opened investigation OIG-557 on January 28, 2011, in response to an anonymous complaint alleging mismanagement of a computer security lab in the Division of Trading and Markets Automation Review Policy (ARP) program. The computer security lab, known as the ARP lab, is used to support the Division of Trading and Markets Office of Market Continuity inspection program, commonly referred to as the ARP program, which inspects self-regulatory organization (SRO), stock exchange (exchange), and clearing agency computer networks.[1]

The anonymous complaint alleged that ARP lab staff and management inappropriately allocated and spent significant budget dollars to purchase computer equipment for the lab without justification or planning; used unencrypted laptops during inspections, in violation of SEC information technology security policies; and inappropriately used SEC funds for training without filing appropriate training forms. Also included in the anonymous complaint were allegations regarding unprofessional behavior, ineffective management, and misuse of unrestricted Internet access.

1. Violations of Acquisition Policy

In its investigation, the OIG found that ARP lab staff spent over a million dollars on computer equipment and software with little oversight or planning and that much of the equipment and software purchased was unneeded or never used in the inspection program. The OIG found that some of the equipment was taken home by employees and used primarily for personal purposes. The OIG also found that some of the equipment was purchased under false pretenses. Two members of the lab staff admitted to misrepresenting in contracting documents that the lab needed (b)(7)(E) laptops because the entities they were inspecting were commonly using (b)(7)(E) products and that (b)(7)(E) were needed for (b)(7)(E) (b)(7)(E) However, the OIG found that (b)(7)(E) products were not commonly used at

[1] For purposes of this report, the terms SRO and exchange are sometimes used individually to refer to the entities inspected by the ARP program. For more information on the entities the ARP program inspects, *see* http://intranet.sec.gov/knowledge_center/markets_and_sros/exchange_sro_websites.html.

This document is subject to the provisions of the Privacy Act of 1974, and may require redaction before disclosure to third parties. No redaction has been performed by the Office of Inspector General. Recipients of this report should not disseminate or copy it without the Inspector General's approval.

the entities the lab staff inspected and that (b)(7)(E) cannot be used for (b)(7)(E) because they have no (b)(7)(E). Moreover, the OIG found that the ARP program had stopped performing (b)(7)(E) before the (b)(7)(E) were ordered.

2. Violations of Information Technology Security Policy

The OIG further learned during the investigation that ARP lab staff were taking unencrypted laptops and laptops without virus protection on inspections and (b)(7)(E) (b)(7)(E) laptops (b)(7)(E) (b)(7)(E)

Because the laptops used by ARP lab staff were not configured by the SEC's Office of Information Technology (OIT), the lab staff were responsible for installing and maintaining encryption and antivirus software on those laptops. However, several laptops had no such protection and the lab had no internal policies about installing or maintaining encryption and virus protection on the lab equipment despite an SEC-wide requirement that all portable media, including laptops, contain encryption. In addition, because lab staff had administrative rights to the laptops they used, they could turn off installed protection at any time. The OIG found that in one instance a computer initially identified to the OIG as having encryption software did not have encryption turned on when the computer was taken on inspections. The user of this computer admitted in testimony that he turned on the encryption only for the purpose of providing the encryption information to the OIG.

Although no lab laptop was reported lost or stolen, any of the unprotected laptops could have been compromised. The OIG found evidence that the unprotected laptops were left unattended in hotel rooms and in offices outside the SEC. The laptops were connected to public wireless networks at hotels and may also have been taken (b)(7)(E) In addition, lab staff took the laptops (b)(7)(E) (b)(7)(E)

(b)(7)(E)

The OIG also found that the laptops and the data they contained were placed at risk when they were connected to an unfiltered, unmonitored (b)(7)(E) Internet connection in the lab. ARP lab staff used that connection to access Internet sites otherwise prohibited by SEC OIT policy, such as personal e-mail sites. The staff also used the lab Internet to download freeware onto the unprotected laptops in violation of SEC OIT policy, and then used those laptops to (b)(7)(E) (b)(7)(E) Lab staff, including a manager, also brought in personal computers, which were connected to the lab network, potentially infecting that network

(b)(7)(E)

This document is subject to the provisions of the Privacy Act of 1974, and may require redaction before disclosure to third parties. No redaction has been performed by the Office of Inspector General. Recipients of this report should not disseminate or copy it without the Inspector General's approval.

with viruses and malware. Further, in violation of SEC OIT policy, an employee used his personal e-mail accounts (b)(7)(E) (b)(7)(E)

3. Violations of Training Policy

The OIG found that the lab staff's multiple violations of SEC OIT security policies occurred despite the fact that the SEC spent hundreds of thousands of dollars training the lab staff. The ARP lab had perhaps the largest per person training budget at the SEC, spending, with little oversight, an average of $20,000 on training per person per year and as much as $30,000 on a single person in a given year. Lab staff could choose from a variety of classes offered by prepaid training vendors and sign up for those classes without filling out training forms usually required for other SEC staff. One member of the lab staff was able to take the same class twice without management's knowledge or approval.

Lab staff were also not required to sign continued service agreements in conjunction with their training. Therefore, they were able to leave the SEC any time after building up their resumes with tens of thousands of dollars in training paid for by the SEC. One staff member left after receiving almost $50,000 worth of training over a four-year period.

The OIG found that lab management did very little to monitor what was happening in the lab. Management could not physically access the lab with their badges for several years, did not know what equipment the lab purchased or what it was used for, and did not track or monitor the training that lab staff received. Management also did not put in place policies and procedures to protect SRO, exchange, and clearing agency data collected by lab staff or take any steps to ensure that lab staff were abiding by SEC OIT policies.

SEC management has already commenced certain actions to address the problems and deficiencies identified by our investigation. Specifically, to determine whether (b)(7)(E) (b)(7)(E) OIT has contracted with an outside forensics team to conduct testing on selected laptops that had been used by the ARP lab. Division of Trading and Markets management has also implemented several policy changes within the ARP lab. Further, management placed two of the lab staff members on administrative leave pending the completion of the OIG's investigation into whether they improperly used government-furnished equipment and failed to adequately safeguard sensitive information. Subsequently, the SEC's Branch Chief for Personnel Security Operations notified these two individuals of a tentative determination to revoke their eligibility for access to classified information and/or occupancy of a sensitive position. Thereafter, both individuals resigned from their SEC employment.

The OIG is referring this report of investigation to management for consideration of appropriate administrative action for the managers and employees responsible for the violations and deficiencies described in this report who remain employed by the SEC. The OIG further recommends that OIT exercise authority over the ARP lab to ensure that lab equipment is properly secured and accounted for, encryption and virus protection are installed on all computers, and the lab Internet connection is properly filtered and monitored.

This document is subject to the provisions of the Privacy Act of 1974, and may require redaction before disclosure to third parties. No redaction has been performed by the Office of Inspector General. Recipients of this report should not disseminate or copy it without the Inspector General's approval.

The OIG additionally recommends that the ARP lab's future equipment purchases be monitored by another SEC office that has sufficient knowledge to determine whether purchases are cost-effective and appropriate for the lab's mission.

The OIG also recommends that lab staff be required to fill out appropriate forms, such as Standard Form 182 (SF-182), Authorization, Agreement and Certification of Training, before enrolling in any training, including prepaid vendor training, in order to properly document the approval process for each training class taken by lab staff. The OIG further recommends that the SEC clarify its policy on continued service agreements and consider requiring all SEC employees to sign continued service agreements prior to enrolling in training that costs more than $5,000.

Finally, we are providing this report to the OIG Office of Audits for consideration of conducting follow-up audits of the ARP lab and, more broadly, of the purchase of information technology equipment throughout the SEC to ensure that proper controls are in place to prevent waste and potential data breaches in the future.

Scope of the Investigation

The OIG obtained and reviewed the e-mail records covering the period from March 1, 2008, to October 31, 2011, of eight current and former SEC employees who worked in the ARP lab. The OIG also reviewed numerous documents pertaining to the lab, including records of equipment purchased by the lab, training classes attended by lab personnel, and screen-shots of lab laptop computers.

The OIG took on-the-record, under-oath the testimony of the following individuals:

1. (b)(6),(b)(7)(C) Division of Trading and Markets, SEC; taken on May 27, 2011 (b)(6),(b)(7)(C) Testimony Tr.). Excerpts of testimony transcript attached at Exhibit 1. (b)(6),(b)(7)(C) left the SEC (b)(6),(b)(7)(C))

2. (b)(6),(b)(7)(C) Office of Information Technology, SEC; taken on December 16, 2011 (b)(6),(b)(7)(C) Testimony Tr.). Excerpts attached at Exhibit 2.

3. (b)(6),(b)(7)(C) Office of Information Technology, SEC; taken on January 9, 2012 (b)(6),(b)(7)(C) Testimony Tr.). Excerpts attached at Exhibit 3. (b)(6),(b)(7)(C) left the SEC (b)(6),(b)(7)(C))

4. (b)(6),(b)(7)(C) Office of Financial Management, SEC; taken on February 6, 2011 (b)(6),(b)(7)(C) Testimony Tr.). Excerpts attached at Exhibit 4.

5. (b)(6),(b)(7)(C) Office of Compliance Inspections and Examinations, Philadelphia Regional Office, SEC; taken on February 17, 2012 (b)(6),(b)(7)(C) Testimony Tr.). Excerpts attached at Exhibit 5.

This document is subject to the provisions of the Privacy Act of 1974, and may require redaction before disclosure to third parties. No redaction has been performed by the Office of Inspector General. Recipients of this report should not disseminate or copy it without the Inspector General's approval.

6. [redacted] SEC University, SEC; taken on February 6, 2012 [redacted] Testimony Tr.). Excerpts attached at Exhibit 6.

7. [redacted] Division of Trading and Markets, SEC; taken on March 19, 2012 [redacted] Testimony Tr.). Excerpts attached at Exhibit 7.

8. [redacted] of Trading and Markets, SEC; taken on March 19, 2012 ([redacted] Testimony Tr.). Excerpts attached at Exhibit 8. [redacted] resigned from the SEC [redacted].)

9. [redacted] Division of Trading and Markets, SEC; taken on May 27, 2011 ([redacted] Testimony Tr.). Excerpts attached at Exhibit 9. [redacted] resigned from the SEC [redacted] [redacted]

10. [redacted] Division of Trading and Markets, SEC; taken on April 9, 2012 [redacted] Testimony Tr.). Excerpts attached at Exhibit 10. [redacted] retired from the SEC [redacted].)

11. [redacted] Office Head, Division of Trading and Markets, SEC; taken on April 9, 2012 [redacted] Testimony Tr.). Excerpts attached at Exhibit 11.

12. [redacted] Information Technology Specialist, Division of Trading and Markets, SEC; taken on May 18, 2012 [redacted] Testimony Tr.). Excerpts attached at Exhibit 12.

Relevant Statutes, Regulations, and Policies

I. Commission Conduct Regulation

The Commission's Regulation Concerning Conduct of Members and Employees of the Commission (Conduct Regulation), at 17 C.F.R. §§ 200.735-1 *et seq.*, sets forth the standards of ethical conduct required of Commission members and employees. The Conduct Regulation states, in part, the following:

> The Securities and Exchange Commission has been entrusted by Congress with the protection of the public interest in a highly significant area of our national economy. In view of the effect which Commission action frequently has on the general public, it is important that . . . employees . . . maintain unusually high standards of honesty, integrity, impartiality and conduct. . . . [and] be constantly aware of the need to avoid situations which might

This document is subject to the provisions of the Privacy Act of 1974, and may require redaction before disclosure to third parties. No redaction has been performed by the Office of Inspector General. Recipients of this report should not disseminate or copy it without the Inspector General's approval.

> result either in actual or apparent misconduct or conflicts of interest. . . .

17 C.F.R. § 200.735-2.

The Conduct Regulation further states, in part, the following:

> ...[A] member or employee should avoid any action...which would result in or might create appearance of, among other things: (i) Using public office for private gain... or (v) Affecting adversely the confidence of the public in the integrity of the Government....

17 C.F.R. § 200.735-3.

II. SEC OIT Rules of the Road

The SEC OIT Rules of the Road apply to all users of SEC information technology resources. The rules state, in relevant part, the following:

Rule #2: Don't Abuse the Privilege of Using the Internet/Intranet

. . . .

- DO NOT download or install any software from the Internet. This includes freeware, shareware, public domain software, Web plug-in software such as video players, video streaming software, sound recorders/players, MP3 music files or any instant messaging (IM) software. . . .
- DO NOT use any Internet-based e-mail accounts from SEC computers while at work or home or on travel unless authorized by OIT in the course of your duties. This includes e-mail portals such as Hotmail, MSN, Yahoo, AOL, etc.
- DO NOT download any files that violate copyright laws for personal use (e.g., MP3 music files, video or computer games). . . .

Rule #7: Don't Transmit Non-public or Sensitive Information over Non-secure Systems

. . . .

- DO NOT transmit non-public information or sensitive data through the Internet or via e-mail, unless you have encrypted it using the SEC's approved encryption software.
- DO NOT store or transmit non-public information or sensitive data on SEC IT resources without proper protection/encryption.
- DO NOT leave laptop computers containing non-public information or sensitive data unprotected. . . .

Rule #9: Protect SEC Network and Automated System Assets

. . . .

This document is subject to the provisions of the Privacy Act of 1974, and may require redaction before disclosure to third parties. No redaction has been performed by the Office of Inspector General. Recipients of this report should not disseminate or copy it without the Inspector General's approval.

- DO NOT install or use any commercial, personally owned, public domain, freeware or shareware software on any SEC computer. . . .

SECR 24-04.A01, Rules of the Road (Version 7.0), March 16, 2011.

III. SEC Encryption Policy

SEC OIT Implementing Instruction, Encrypting Data on Portable Media, II 24-04.04.05 (02.0), dated December 1, 2010 (initially issued April 6, 2010), Section 5, requires that the local hard drive on all SEC laptop computers be encrypted using SEC-approved information encryption (SAIE) software before the computers are issued to end users. This policy section also requires that all sensitive, nonpublic, and personally identifiable information (PII) data on portable media be encrypted. The definition of portable media includes laptop computers.

IV. SEC Training and Development Policy

The SEC's Training and Development Policy, issued June 22, 2007, states, in part, the following under paragraph 5.1, Requesting Internal Courses:

> To register for any internal course an employee must:
>
> - obtain permission from the immediate and 2nd level supervisors prior to registering . . . .

Internal courses are defined in the policy, at paragraph 1.1, as "[a]ll courses provided directly by the SEC or by organizations under contract to the SEC." *Id.* at paragraph 1.1

In addition, paragraph 11.0 of the policy, Continued Service Agreement for Training, provides that, in accordance with 5 U.S.C. § 4108, "the SEC reserves the right to require an employee to sign a continued service agreement prior to attending a course." This paragraph further states as follows:

> An SEC employee selected for a course that extends over more than 60 calendar days and take[s] place during normal work hours, and/or if the cost of the course is $5,000 or more (including all authorized expenses) regardless of length shall agree in writing, before assignment to the course, that the employee will:
>
> - continue in the service of the Government after the completion of the course for a period of one year, unless involuntarily separated from the service of the Government; and will
> - pay expenses related to instruction incurred by the Government if voluntarily separated from Government service before the end of the agreed period of service.

Id. at paragraph 11.0 (footnote omitted).

This document is subject to the provisions of the Privacy Act of 1974, and may require redaction before disclosure to third parties. No redaction has been performed by the Office of Inspector General. Recipients of this report should not disseminate or copy it without the Inspector General's approval.

Results of the Investigation

I. Creation and Staffing of the ARP Lab

In 2005, the Division of Trading and Markets' ARP program created a computer security lab to address a Government Accountability Office (GAO) recommendation that the Division of Trading and Markets staff become more technologically proficient, especially in information security.[3] (b)(6),(b)(7)(C) Testimony Tr. at 13-15. Although GAO did not specifically recommend creation of a lab, the lab was intended to enable Division of Trading and Markets staff to acquire, test, and understand technologies used in the industry. *Id.* at 15. The ARP lab was initially set up on the sixth floor [of Station Place I at SEC headquarters]. (b)(6),(b)(7)(C) Testimony Tr. at 11. For several years, the ARP lab staff consisted of (b)(6),(b)(7)(C), and a varying fourth person who "drift[ed] in and out." (b)(6),(b)(7)(C) Testimony Tr. at 17.

(b)(6),(b)(7)(C) was one of the first ARP program staff assigned to the lab and helped "pitch the concept" of the lab to management. *Id.* at 13. (b)(6),(b)(7)(C) did not have a technical background but had a public policy degree from Carnegie Mellon University (Carnegie Mellon) and had been working in the ARP program (b)(6),(b)(7)(C) *Id.* at 7-8. (b)(6),(b)(7)(C) reported to (b)(6),(b)(7)(C) (b)(6),(b)(7)(C), who had been in the ARP program (b)(6),(b)(7)(C) Testimony Tr. at 7-8. (b)(6),(b)(7)(C) reported to (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) ARP program and had been with the SEC (b)(6),(b)(7)(C) Testimony Tr. at 7, 9-11. Neither (b)(6),(b)(7)(C) nor (b)(6),(b)(7)(C) had any technical knowledge of SRO systems.[5] (b)(6),(b)(7)(C) Testimony Tr. at 6-7; (b)(6),(b)(7)(C) Testimony Tr. at 7.

(b)(6),(b)(7)(C) was hired in (b)(6),(b)(7)(C) as an (b)(6),(b)(7)(C) for the ARP program. (b)(6),(b)(7)(C) Testimony Tr. at 11-12. He was assigned to the lab and reported to (b)(6),(b)(7)(C) *Id.* at 12. (b)(6),(b)(7)(C) had attended Carnegie Mellon with (b)(6),(b)(7)(C) who recruited (b)(6),(b)(7)(C) for the position in the ARP program. (b)(6),(b)(7)(C) Testimony Tr. at 19. (b)(6),(b)(7)(C) was also hired in (b)(6),(b)(7)(C) as an (b)(6),(b)(7)(C) assigned to the lab and reporting to (b)(6),(b)(7)(C) Testimony Tr. at 6-7. (b)(6),(b)(7)(C) was hired just after he had (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) and had little technical experience. *Id.* at 6.

(b)(6),(b)(7)(C) was promoted to a newly created (b)(6),(b)(7)(C) position for the ARP program, putting him in charge of the ARP lab. (b)(6),(b)(7)(C) Testimony Tr. at 13-14. (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) was again promoted, this time to a newly created nonsupervisory position of

---

[3] In 2005, the Division of Trading and Markets was called the Division of Market Regulation. The SEC's ARP program, also known as the Office of Market Continuity, was created in 1989 to address operational risks at SROs, exchanges, and clearing agencies. As part of the program, the SROs, exchanges, and clearing agencies voluntarily submit to periodic on-site review by ARP staff, who assess selected information technology or operational issues. In 2003 and 2004, GAO issued two reports, GAO-03-414 and GAO 04-984, recommending that the SEC improve the effectiveness of the ARP program and expand the level of staffing and resources committed to the program.

[4] (b)(6),(b)(7)(C) retired from the SEC (b)(6),(b)(7)(C)

[5] Initially after the GAO recommendation, contractors were hired to provide technical expertise at inspections; however, the contractors were expensive and management determined that hiring in-house experts would be more cost-effective. (b)(6),(b)(7)(C) Testimony Tr. at 19-20.

This document is subject to the provisions of the Privacy Act of 1974, and may require redaction before disclosure to third parties. No redaction has been performed by the Office of Inspector General. Recipients of this report should not disseminate or copy it without the Inspector General's approval.

[redacted], and [redacted] assumed the [redacted] that [redacted] had held. [redacted] Testimony Tr. at 13; [redacted] Testimony Tr. at 10.

[redacted] before [redacted] took over as [redacted] was hired as an [redacted] assigned to the ARP lab. [redacted] Testimony Tr. at 11-12. [redacted] at [redacted] as [redacted] and had remained friends with [redacted] *Id.* Although [redacted] had worked in systems management, he had no experience working with the SRO systems inspected by the ARP lab. *Id.* at 10-11. In [redacted] was promoted to [redacted] along with [redacted] [as [redacted] had left the SEC]. *Id.* at 13.

[redacted] was hired as an [redacted] in the ARP lab in [redacted] Testimony Tr. at 6-7. [redacted] had experience working with UNIX systems [redacted] *Id.* at 6. However, he too had no SRO experience and was surprised to learn that his duties at the SEC included "going out to exchanges for auditing IT controls."[6] *Id.* at 8.

According to [redacted] the ARP lab was set up to "beef up the Trading and Markets technical staff." [redacted] Testimony Tr. at 67. However, the OIG found that the lab staff remained primarily a small group of only four to five people, most of whom lacked industry-specific technical skills.

II. [redacted] and [redacted] Did Not Adequately Supervise the ARP Lab

The OIG found that during the period when the ARP lab was located on the sixth floor of Station Place I, from its creation in 2006 until its move to the seventh floor of Station Place II in the fall of 2011, neither [redacted] nor [redacted] had card key access to the lab even though they supervised the lab and all of its employees. [redacted] Testimony Tr. at 17; [redacted] Testimony Tr. at 23-25. [redacted] testified that only he, [redacted] and [redacted] had access to the lab and that [redacted] even though he was the "boss for everything," did not get card key access to the lab until the beginning of 2012. [redacted] Testimony Tr. at 22. When he was asked why [redacted] did not have access to the lab he supervised, [redacted] responded that [redacted] "doesn't use the lab." In addition, he said, [redacted] only got card key access because ARP staff members who could not access the lab had complained and the decision was made that all ARP staff and managers should have access to the lab after it moved to the seventh floor. *Id.* at 23-25.

---

[6] Currently, the ARP inspection program is voluntary for SROs. However, the Division of Trading and Markets is in the process of drafting a rule that would make compliance with ARP standards mandatory. SEC Chairman Mary Schapiro announced this effort in a speech to the Securities Industry and Financial Markets Association (SIFMA) in March 2011. The rule would call for market participants to satisfy requirements for the capacity, resiliency, and security of their automated systems. Mary Schapiro, Chairman, SEC, Remarks at SIFMA's Compliance and Legal Society Annual Seminar (Mar. 23, 2011), available at http://www.sec.gov/news/speech/2011/spch032311mls.htm. GAO recommended this change in its 2004 Financial Market Preparedness Report, citing the need for greater assurance that organizations will continue to comply with ARP recommendations. GAO, *Financial Market Preparedness: Improvements Made, but More Action Needed to Prepare for Wide-Scale Disasters,* GAO-04-984, (Sept. 27, 2004), at 31, available at http://www.gao.gov/new.items/d04984.pdf. The rule is currently in draft form and has not yet been published for general comment.

This document is subject to the provisions of the Privacy Act of 1974, and may require redaction before disclosure to third parties. No redaction has been performed by the Office of Inspector General. Recipients of this report should not disseminate or copy it without the Inspector General's approval.

(b)(6),(b)(7)(C) also testified that he did not get card key access to the lab until after the lab had moved to the seventh floor. (b)(6),(b)(7)(C) Testimony Tr. at 11. He said that if he wanted to enter the lab before that move, he "needed (b)(6),(b)(7)(C) or (b)(6),(b)(7)(C) or (b)(6),(b)(7)(C) to let him in. *Id.* (b)(6),(b)(7)(C) said that there was "no particular reason" he did not have card key access to the lab and that he did not think the lack of card key access made it hard for him to supervise the lab staff because he is "not a day-to-day guy" and "not that hands-on." *Id.* at 11-12.

(b)(6),(b)(7)(C) testified that he was unaware that he did not have card key access to the lab when it was on the sixth floor, stating, "I presume I have had [access] all along . . . since the beginning." (b)(6),(b)(7)(C) Testimony Tr. at 13. However, when (b)(6),(b)(7)(C) was asked whether he had ever used his badge to get into the lab, he could not provide a specific answer and instead said, "I would have nothing to do in there by myself. I would not go in there unless there's—I'm going in with somebody." *Id.* (b)(6),(b)(7)(C) also testified that he did not know that (b)(6),(b)(7)(C) could not access the lab on the sixth floor, saying, "I can't imagine him not having [access]." *Id.* at 14.

Even if (b)(6),(b)(7)(C) thought he could access the lab (b)(6),(b)(7)(C) testified that he spent "very little" time in the lab—"less than 10 minutes a week." *Id.* at 12-13. (b)(6),(b)(7)(C) likewise testified that "not much" of his time was spent in lab. (b)(6),(b)(7)(C) Testimony Tr. at 11. Lab staff confirmed that (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) did not spend much time in the lab. (b)(6),(b)(7)(C) Testimony Tr. at 21; (b)(6),(b)(7)(C) Testimony Tr. at 13. (b)(6),(b)(7)(C) said that he believed "nobody" supervised his work in the lab. (b)(6),(b)(7)(C) Testimony Tr. at 21-22.

III. ARP Lab Staff Spent Significant Budget Dollars With Little Oversight on Computer Equipment and Software That Were Never Used in the ARP Program

The anonymous complaint to the OIG alleged that (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) had inappropriately allocated and spent significant budget dollars to purchase computer equipment for the ARP lab with no justification or planning and that lab staff were allowed to purchase "whatever equipment [met] their fancy and whim," including the "latest tech toys for their personal use." *See* Anonymous Complaint, attached at Exhibit 11.

In its investigation, the OIG found that ARP lab staff spent hundreds of thousands of dollars on computer equipment and software and that no checks were in place to ensure that the equipment and software purchased were needed or used to further the ARP program mission. In addition, the OIG found that a significant portion of the equipment and software purchased was never used in the ARP program.

This document is subject to the provisions of the Privacy Act of 1974, and may require redaction before disclosure to third parties. No redaction has been performed by the Office of Inspector General. Recipients of this report should not disseminate or copy it without the Inspector General's approval.

A. The SEC's Project Review Board Approved More Than a Million Dollars for Equipment and Software for the ARP Lab Without Sufficient Information on How the Money Was to Be Spent

Each year, ARP lab staff went before the SEC's Information Technology Project Review Board (PRB) to request money to purchase computer equipment and software for the lab.[7] (b)(6),(b)(7)(C) Testimony Tr. at 26. The lab staff would draft an Information Technology Investment Plan (Investment Plan) and submit it to PRB and would make a presentation to PRB requesting funds. (b)(6),(b)(7)(C) Testimony Tr. at 71, 74.

(b)(6),(b)(7)(C) said that he played a "support" role in the process, helping (b)(6),(b)(7)(C) develop the information to be submitted to PRB. (b)(6),(b)(7)(C) Testimony Tr. at 26-27. (b)(6),(b)(7)(C) testified that he "helped create" the Investment Plans and that he did "most" of the speaking at PRB meeting presentations, with (b)(6),(b)(7)(C) sometimes also speaking. (b)(6),(b)(7)(C) Testimony Tr. at 74, 78.

The OIG obtained the Investment Plans that ARP lab staff submitted to PRB for 2006 through 2010. During that five-year period, the ARP Lab submitted and received approval for requests totaling $1,179,933. *See* Information Technology Investment Plans 2006-2010, attached at Exhibit 14. The 2006 and 2010 Investment Plans included information on specific hardware and software the lab staff planned to buy. *Id.* The other three Investment Plans, however, did not have any specific items listed. *Id.* None of the lab staff could explain why the 2007, 2008, and 2009 Investment Plans submitted to PRB did not have specific information on how the lab staff planned to spend the money requested. (b)(6),(b)(7)(C) Testimony Tr. at 109-110, (b)(6),(b)(7)(C) Testimony Tr. at 28, (b)(6),(b)(7)(C) Testimony Tr. at 23. When asked why some Investment Plans did not have specific items listed, (b)(6),(b)(7)(C) said, "I don't know . . . sometimes they ask you to and sometimes they don't." (b)(6),(b)(7)(C) Testimony Tr. at 28.

(b)(6),(b)(7)(C) a member of PRB from 2001 to 2011, said that he did not remember reviewing the lab's Investment Plans and did not specifically remember any presentations the lab staff made to PRB. (b)(6),(b)(7)(C) Testimony Tr. at 7-8, 15. When asked what he knew about the ARP lab (b)(6),(b)(7)(C) said, "Not a lot, to be honest." *Id.* at 11. (b)(6),(b)(7)(C) was able to explain that the ARP program was "set up to do reviews of the SRO [trading technology and designed] to give the Agency some understanding of what the SROs were doing as far as developing their systems and protecting those systems." *Id.* But, he said, "I don't know much more about that." *Id.* (b)(6),(b)(7)(C) said that PRB was not involved in any of the policy decisions to set up the lab or in "the specific configuration of it." *Id.* at 13. According to (b)(6),(b)(7)(C) PRB's role was only to consider "new technology investments." *Id.* at 12.

(b)(6),(b)(7)(C) said that PRB did not require "laundry lists of stuff" in order to approve a project. *Id.* at 18. In addition, (b)(6),(b)(7)(C) said that after a project was approved by PRB, no one checked to

[7] In his OIG testimony, long-time PRB member (b)(6),(b)(7)(C) explained that PRB functions to fulfill a Clinger-Cohen Act requirement that "senior level people in an agency be involved in [information technology] buys." (b)(6),(b)(7)(C) Testimony Tr. at 26. *See also* Clinger-Cohen Act, 40 U.S.C § 11101 *et seq.*, available at http://www.cio.gov/Documents/it_management_reform_act_feb_1996.html. The PRB role and composition are described in its charter, 24-02-PRB-01, issued February 22, 2012 (formerly OD24-02.01.C03).

This document is subject to the provisions of the Privacy Act of 1974, and may require redaction before disclosure to third parties. No redaction has been performed by the Office of Inspector General. Recipients of this report should not disseminate or copy it without the Inspector General's approval.

see what items were actually bought. *Id.* at 18-19. He said that PRB was supposed to receive "status reports" on projects but "that process did not always work terribly well." *Id.* at 20. Further, he said that when PRB did get status reports, they lacked any detail. *Id.* at 22. However, according to (b)(6),(b)(7)(C) performing checks on how programs spend their PRB-approved budgets is not PRB's role and PRB does not have the resources to do more that it does. *Id.* at 22, 24.

(b)(6),(b)(7)(C) further explained, "One of the frustrations of being on the PRB over the many years was the inability to get as much information as we wanted on a lot of projects." *Id.* at 19. (b)(6),(b)(7)(C) said he had "some discomfort" with the fact that he did not have a good sense of what the ARP lab was buying and what it was using its purchases for. *Id.* at 52-53. In his testimony, (b)(6),(b)(7)(C) stated that he was concerned that ARP lab staff were purchasing "BSOs" instead of what they actually needed for the lab:

> There is a term in the technology world call BSOs, which are bright, shiny objects, which comes from the concept of magpies, want to pick up bright, shiny objects to take back to their nests. Well, you get a group of IT people together and they're always playing with some new, bright, shiny object. Well, particularly those of us who are non-technology people used to joke about that as being, you know, kind of the lure, the draw for a lot of the technology folks, particularly those who are wire-head types who get into labs, like the forensics labs, and the ARP Labs. They're going to be very attracted to bright, shiny objects. So, yeah, we always talked about them wanting to play with the latest toys.

Id. at 46-47.

(b)(6),(b)(7)(C) confirmed in his testimony that no one from the ARP program went back to PRB to inform it of what was purchased: "You don't circle back and say, okay this is what I bought, exactly line by line you don't. At least we've never done it." (b)(6),(b)(7)(C) Testimony Tr. at 35. (b)(6),(b)(7)(C) also could not identify an occasion on which PRB was specifically informed of the items purchased by the ARP lab.[8] (b)(6),(b)(7)(C) Testimony Tr. at 92-93. (b)(6),(b)(7)(C) testified that he "tried to keep people involved" but did not know of a "formal process" to do so. *Id.* at 93.

[8] (b)(6),(b)(7)(C) mentioned in testimony that OIT staff member (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) visited the lab on one occasion and was shown some equipment purchased by the lab. (b)(6),(b)(7)(C) Testimony Tr. at 93. However, (b)(6),(b)(7)(C) testified that in his one visit to the lab he "didn't verify anything." (b)(6),(b)(7)(C) Testimony Tr. at 35. The SEC's (b)(6),(b)(7)(C), also a member of PRB, visited the lab in 2009, but he testified that he only saw "a lot of things in boxes." (b)(6),(b)(7)(C) Testimony Tr. at 11-12, 33.

This document is subject to the provisions of the Privacy Act of 1974, and may require redaction before disclosure to third parties. No redaction has been performed by the Office of Inspector General. Recipients of this report should not disseminate or copy it without the Inspector General's approval.

B. OIT Did Not Adequately Supervise the ARP Lab's Equipment and Software Orders

After PRB approved project funding for the ARP lab, lab staff worked with OIT staff, usually [redacted] to purchase the specific equipment and software for the lab.[9] [redacted] Testimony Tr. at 16-17. [redacted] testified that starting in 2005, he worked with the ARP lab staff as their OIT liaison. [redacted] Testimony Tr. at 8. [redacted] said that [redacted] or [redacted]'s staff would fill out a procurement request (PR) and send it to him, usually by e-mail. *Id.* at 25, 27. [redacted] said that he would then look at the PR and verify that it contained the correct budget object class (BOC) code and that there was funding for that BOC code. *Id.* at 25-26. [redacted] said that the BOC codes covered broad categories such as software, hardware, and consulting services. *Id.* at 25.

[redacted] described OIT's role in the ARP lab as "very minimal," noting that the lab "wasn't an OIT project." *Id.* at 9-10. [redacted] said the lab was "external" to OIT and that OIT's role was "just to make sure the [lab's] money followed through the capital client process." *Id.* at 10. [redacted] said that once the money was approved, he would make sure that "the money [was] in the right category . . . [a]nd that was pretty much the extent of [his] involvement, other than making sure they completed all the necessary documentation." *Id.* at 12.

[redacted] said that the amount of hardware the lab was buying piqued his curiosity but that he could not "ascertain whether it was valid or not" and "didn't have the authority to do anything, really." *Id.* at 22. [redacted] said that he could not determine whether it was cost-effective for the lab to purchase particular hardware or whether an expenditure was worthwhile. *Id.* at 29-30 [redacted] further said that he did not check to see if the lab staff had approval to buy a specific item and that he had no information on what they owned or had bought in the past because he never saw the invoices. *Id.* at 30, 35. He said that he did not look at the Investment Plans that were submitted to PRB to see what was in the plans. *Id.* at 31. After he received a PR, [redacted] would forward it to someone else in OIT in the finance and budgeting office, who would verify that funding was available. *Id.* The person to whom he forwarded the PR also took no action to ascertain whether the expenditure was appropriate and not wasteful. *Id.* at 32. [redacted] said that the requisition information would then go into a computer system and a contracting officer in the Office of Financial Management would process the order and [again] "just verify that there was money."[10] *Id.* at 33. [redacted] testified that he "absolutely" had concerns about ordering equipment for a division outside of OIT and about being involved in a process in which he was not in a position to determine whether the purchases were appropriate. *Id.* at 34.

---

[9] [redacted] left the SEC [redacted] Testimony Tr. at 6-7. [redacted] *Id.* at 7. During that time, [redacted] also served on PRB [redacted] *Id.* at 14. [redacted] said he did not recall ever reviewing a proposal from the ARP lab. *Id.*

[10] The OIG interviewed [redacted], a contracting officer who processed several contracts for the ARP Lab. She confirmed that the contracting officers only obligate money in contracts with vendors and do not otherwise ask questions. She said that by the time the request gets to her, she assumes it has already been approved by management.

This document is subject to the provisions of the Privacy Act of 1974, and may require redaction before disclosure to third parties. No redaction has been performed by the Office of Inspector General. Recipients of this report should not disseminate or copy it without the Inspector General's approval.

The SEC's (b)(6),(b)(7)(C) who served on PRB at the time of one of the ARP lab's budget requests, also testified about his concerns related to the ARP lab. (b)(6),(b)(7)(C) referred to the lab as "a toy box" and said that he was "not comfortable" that the procurement process had to go through OIT because OIT had "no idea whether [the items purchased are] being used and how they're being used." (b)(6),(b)(7)(C) Testimony Tr. at 36-37. (b)(6),(b)(7)(C) testified that he was in the process of trying to get the ARP lab "removed out" of his "budget line item." *Id.* at 38.

C. (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) Did Not Provide Meaningful Input to the Budget or Purchasing Process

The OIG found that the ARP lab's own management, like PRB and OIT, did not act as an adequate check on the lab's purchasing. In the case of the lab's management, this failure resulted from both a lack of involvement in the lab and insufficient technical knowledge.

For example (b)(6),(b)(7)(C) seemed uncertain about how the PRB budget process worked, testifying that he thought that lab staff went to PRB every time they wanted to buy a single piece of equipment (b)(6),(b)(7)(C) Testimony Tr. at 21 (b)(6),(b)(7)(C) testified that he went to a PRB meeting "once or twice" but that he could not remember the years of those meetings or who from his staff gave the presentation at the meetings. *Id.* at 35-36 (b)(6),(b)(7)(C) also said he did not know who from his staff drafted the Investment Plans that were submitted to PRB. *Id.* at 36.

(b)(6),(b)(7)(C) testified that although he thought he "probably" talked to his staff about what they wanted to purchase, he did not have a sufficient technical background to weigh in on the specifics and never told his staff that they could not purchase something because "[he] presumed that all of these people understood it better than [he] did." *Id.* at 39-40. (b)(6),(b)(7)(C) said that he did not know how much the lab spent each year on computer equipment. *Id.* at 40. He said that he thought (b)(6),(b)(7)(C) was the "primary person" who ordered equipment for the lab and that (b)(6),(b)(7)(C) "would have consulted with [him]" as well as with (b)(6),(b)(7)(C) *Id.* at 42 (b)(6),(b)(7)(C) said, "I would not use the word he got approval from us, but I was told at the beginning what we were asking for." *Id.* (b)(6),(b)(7)(C) said that he did not see the PRs before they were submitted and did not think that (b)(6),(b)(7)(C) did either. *Id.* at 43 (b)(6),(b)(7)(C) said that he thought the lab staff got approval through "the purchasing people" to buy items for the lab, but that "[t]here is no procedure that [he] know[s] of" within the lab to check on what (b)(6),(b)(7)(C) was ordering. *Id.* at 44.

(b)(6),(b)(7)(C) seemed to know a little bit more about the PRB process than (b)(6),(b)(7)(C) did, stating that the ARP lab went to PRB "once a year" to get authority to have "X dollars set aside for the budget." (b)(6),(b)(7)(C) Testimony Tr. at 27-28. (b)(6),(b)(7)(C) testified that he did not know why some Investment Plans had specific details in them and others did not, but noted that (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) gave presentations to PRB. *Id.* at 22-23.

(b)(6),(b)(7)(C) said that after PRB approved the budget, the lab staff would write up PRs for (b)(6),(b)(7)(C) and that (b)(6),(b)(7)(C) would then approve the purchases. *Id.* at 29-30. However, (b)(6),(b)(7)(C) stated that he did not know what (b)(6),(b)(7)(C) did to approve a purchase, and he acknowledged that (b)(6),(b)(7)(C) was not part of the inspection program and would not be in a position to know what equipment was appropriate for the lab. *Id.* at 30.

This document is subject to the provisions of the Privacy Act of 1974, and may require redaction before disclosure to third parties. No redaction has been performed by the Office of Inspector General. Recipients of this report should not disseminate or copy it without the Inspector General's approval.

(b)(6),(b)(7)(C) testified that (b)(6),(b)(7)(C) ordered the equipment for the ARP lab and that (b)(6),(b)(7)(C) would "not necessarily" run orders by (b)(6),(b)(7)(C) first. *Id.* at 31. (b)(6),(b)(7)(C) also said that he did not review the lab's PRs before they were submitted to (b)(6),(b)(7)(C) *Id.* He further testified that the lab had no internal guidelines as to what lab staff were permitted to buy and that no additional internal review was required for high-cost items. *Id.* 32-33. (b)(6),(b)(7)(C) said that if (b)(6),(b)(7)(C) "could make a verbal argument" as to why the lab needed something, he would say, "[F]ine." *Id.* at 33.

(b)(6),(b)(7)(C) testified that (b)(6),(b)(7)(C) did not get input from (b)(6),(b)(7)(C) when ordering equipment for the lab. (b)(6),(b)(7)(C) Testimony Tr. at 27. He said that because (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) did not have technical knowledge, they had to "rely on the Branch Chief to be able to translate the technical matters" for them, giving (b)(6),(b)(7)(C) a lot of power to make decisions for the lab. *Id.* at 25. (b)(6),(b)(7)(C) testified that in the end it was (b)(6),(b)(7)(C) who decided what would be purchased. *Id.* at 27.

(b)(6),(b)(7)(C) testified that the PRs "had to be approved by (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C)" and initially said that he copied them on the PRs he sent to (b)(6),(b)(7)(C) Testimony Tr. at 84-85. However, when questioned further about whether he copied (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) on all the PRs, (b)(6),(b)(7)(C) said that he did not remember and would have to check his e-mails and then stated, "they knew everything [the lab] bought because it was also done verbally."[11] *Id.* at 86-87.

D. The ARP Lab Purchased Hundreds of Thousands of Dollars' Worth of Equipment and Software Not Used in the ARP Program

The OIG found that the ARP lab purchased hundreds of thousands of dollars' worth of equipment and software that were never used in the ARP program. Some of the more expensive items that were purchased and never used are discussed below.

- (b)(7)(E) software. The ARP lab staff purchased (b)(7)(E) software in 2006 for $29,070. *See* (b)(7)(E) contracting document, attached at Exhibit 15. In addition, the lab staff spent $4,990 to renew the (b)(7)(E) software license in 2007 and $12,000 on (b)(7)(E) training. *See* OIT Chart, attached at Exhibit 16;[12] *see also* (b)(7)(E) Training Contracting Document, attached at Exhibit 17.

  (b)(6),(b)(7)(C) told the OIG that (b)(7)(E) software is a tool used to conduct forensic evaluations and that he remembered taking the (b)(7)(E) training. (b)(6),(b)(7)(C) Testimony Tr. at 43. However, (b)(6),(b)(7)(C) admitted that ARP staff do not do forensic work and said that the lab has "discontinued" (b)(7)(E) because the lab staff "never used it" and "never looked at (b)(7)(E) *Id.* (b)(6),(b)(7)(C) said that the lab purchased (b)(7)(E) because the lab staff were "experimenting with which areas you can go into . . . and that was one of the areas that [they] thought [they] could go into but it never flourished." *Id.* (b)(6),(b)(7)(C)

[11] The OIG's e-mail review showed that (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) were not always copied on e-mails containing outgoing PRs.

[12] The marks and notations on the OIT Chart exhibit were on the document when OIT produced it for the OIG.

This document is subject to the provisions of the Privacy Act of 1974, and may require redaction before disclosure to third parties. No redaction has been performed by the Office of Inspector General. Recipients of this report should not disseminate or copy it without the Inspector General's approval.

was then asked whether he just "experiment[ed] with taxpayer money," and he responded, "No .... That's why we discontinued the product ...." *Id.* at 44.

(b)(6),(b)(7)(C) admitted that purchasing (b)(7)(E) was originally his idea. (b)(6),(b)(7)(C) Testimony Tr. at 96. (b)(6),(b)(7)(C) said that he went to (b)(7)(E) training with (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) and that his initial intent in purchasing (b)(7)(E) was to use it for training because "the exchanges were using (b)(7)(E) " and he wanted to know if they were using it correctly. *Id.* at 96-97. (b)(6),(b)(7)(C) however, could not specifically recall an SRO that had (b)(7)(E) and admitted that he had never inspected any SRO's (b)(7)(E) system. *Id.* at 98. He also acknowledged that ARP lab staff do not do forensics work and that lab staff could have learned about (b)(7)(E) in less costly ways. *Id.* at 100-03.

- (b)(7)(E) The ARP lab purchased (b)(7)(E) in 2006 at a cost of $9,911. *See* OIT Chart. According to (b)(6),(b)(7)(C) it was his idea to purchase this equipment because (b)(7)(E) and he had previously used the equipment when he was at the (b)(7)(E) (b)(6),(b)(7)(C) Testimony Tr. at 106. (b)(6),(b)(7)(C) described the equipment as a (b)(7)(E) (b)(7)(E) that is "used to prevent unwanted folks from (b)(7)(E) (b)(7)(E) *Id.* at 106-07. (b)(6),(b)(7)(C) said the intent in purchasing (b)(7)(E) (b)(7)(E) was not to use it (b)(7)(E) but to use it to (b)(7)(E) (b)(7)(E) at 107. However, (b)(6),(b)(7)(C) admitted that the ARP lab was only beginning to set up a (b)(7)(E) at the time of the purchase, and he could not recall whether (b)(7)(E) was set up during that time.[13] *Id.* at 107-08.

- (b)(7)(E) The ARP lab purchased (b)(7)(E) in 2007 for $72,000. *See* OIT Chart. According to (b)(6),(b)(7)(C) (b)(7)(E) is a vulnerability scanner that looks at feeds from different vulnerability scanners (b)(7)(E) (b)(7)(E) [14] (b)(6),(b)(7)(C) Testimony Tr. at 15. In his OIG testimony, (b)(6),(b)(7)(C) stated that despite the high cost of the equipment, the ARP lab never used (b)(7)(E) (b)(6),(b)(7)(C) Testimony Tr. at 96-97. (b)(6),(b)(7)(C) also confirmed that (b)(7)(E) was never used. (b)(6),(b)(7)(C) Testimony Tr. at 116.

- (b)(7)(E) The ARP lab purchased (b)(7)(E) vulnerability scanning software in 2007 for $40,500. *See* OIT Chart. (b)(6),(b)(7)(C) testified that the lab bought (b)(7)(E) with the idea that the lab would use it on inspections. (b)(6),(b)(7)(C) Testimony Tr. at 111. However, lab staff decided (b)(7)(E) was "not safe to use on inspection[s] because it was overly intrusive." *Id.* (b)(6),(b)(7)(C) testified that he, (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) made the joint decision to purchase (b)(7)(E) and that he does not know where the software is now. *Id.* at 111-12.

---

[13] The OIG noted that (b)(7)(E) is not listed on the Investment Plan for 2006, but the lab was still able to purchase the equipment.

[14] (b)(6),(b)(7)(C) testified that (b)(7)(E) would have to be in place too long and would require too many connections to be valuable in an ARP inspection program. (b)(6),(b)(7)(C) Testimony Tr. at 15-16.

This document is subject to the provisions of the Privacy Act of 1974, and may require redaction before disclosure to third parties. No redaction has been performed by the Office of Inspector General. Recipients of this report should not disseminate or copy it without the Inspector General's approval.

- [redacted]. The ARP lab purchased [redacted] in 2008 for $25,955. *See* OIT chart. According to [redacted] is software that looks for [redacted] Testimony Tr. at 125. [redacted] said that because [redacted] can potentially [redacted] it needed to be configured before it could be used so as not to [redacted] Testimony Tr. at 128. [redacted] said that [redacted] was supposed to configure the software but did not get it to a point where the lab could use it in testing exchanges. [redacted] Testimony Tr. at 128-29. As a result, [redacted] said, it was never used [redacted] *Id.* at 130. [redacted] also remembered the lab purchasing [redacted] and confirmed that it was not used to perform any [redacted] Testimony Tr. at 47-49.

- [redacted] traveling licenses. The ARP lab purchased [redacted] traveling licenses in 2008 for $19,620. *See* OIT Chart. [redacted] told the OIG that [redacted] is vulnerability scanning software and the intention in purchasing it was to "put it on a laptop and use it during an engagement." [redacted] Testimony Tr. at 50. In addition to paying almost $20,000 for [redacted] licenses, the ARP lab spent $16,838 in 2008 on [redacted] training, for a total investment of more than $36,000.[15] *See* OIT Chart. [redacted] said that he, [redacted] and [redacted] took the [redacted] training. [redacted] Testimony Tr. at 107. However, [redacted] said that [redacted] was never deployed. *Id.* at 51. [redacted] confirmed that [redacted] was never implemented, stating that because of a "lack of resources" they "never got around to" using it. [redacted] Testimony Tr. at 134. [redacted] said the decision to buy it "was bad judgment, mistake." *Id.*

In his testimony, [redacted] stated that the ARP lab simply lacked adequate staff or resources to implement the technology purchased and said they "were feeling overwhelmed." *Id.* at 203. When asked why they continued to purchase technology without the resources to implement it, [redacted] said that they had intended to hire more people but acknowledged that buying technology without the resources to implement it was wasting taxpayers' money, albeit "unintentionally." *Id.* at 204.

E. [redacted] and [redacted] Testified That They Did Not Know About the Undeployed Equipment and Software

In an e-mail dated May 9, 2011, addressed to [redacted] and [redacted] informed them that "only 25% of new tools purchased last year have been deployed." *See* E-mail from [redacted] to [redacted] and [redacted] May 9, 2011, attached at Exhibit 18. In the same e-mail, [redacted] mentioned specifically that [redacted][16] [redacted], and [redacted] had not been implemented. *Id.* [redacted] said that he sent the e-mail to [redacted] and [redacted] "to bring to their attention" that the lab

[15] The [redacted] training is listed on the OIT Chart under [redacted]

[16] [redacted] according to [redacted] is a [redacted] Testimony Tr. at 79. [redacted] testified that [redacted] is "an expensive tool" and "to deploy it on all your systems that are nonproduction systems . . . is a bit of a waste." *Id.* at 80. The 2006 Investment Plan lists [redacted] at a cost of $8,071.75. *See* 2006 Investment Plan at 14. The OIT Chart lists an additional investment of approximately $2,000 in [redacted] in 2008. *See* OIT Chart.

This document is subject to the provisions of the Privacy Act of 1974, and may require redaction before disclosure to third parties. No redaction has been performed by the Office of Inspector General. Recipients of this report should not disseminate or copy it without the Inspector General's approval.

staff had "fallen behind" and did not have the resources to implement the tools they were buying. (b)(6),(b)(7)(C) Testimony Tr. at 203-04.

When the OIG asked (b)(6),(b)(7)(C) if he was aware that the lab purchased items that were never used he testified that he was not aware of that and said he "thought they used everything [they] got." (b)(6),(b)(7)(C) Testimony Tr. at 34. Specifically, (b)(6),(b)(7)(C) testified that he was not familiar with (b)(7)(E) and did not know about its purchase or that it was never used. *Id.* (b)(6),(b)(7)(C) testified that while he was familiar with (b)(7)(E) and thought that the ARP lab had used it, he admitted, "We don't do forensics." *Id.* (b)(6),(b)(7)(C) also testified that he had heard of (b)(7)(E) but that he did not know what it does or what it cost and did not specifically authorize its purchase. *Id.* at 37. He also said that he did not know that (b)(7)(E) had not been used and did not know how it would have supported the inspection program if it had been used. *Id.* at 38-39. (b)(6),(b)(7)(C) testified that he was not familiar with (b)(7)(E) or (b)(7)(E) *Id.* at 39. He said he knew that (b)(7)(E) is a vulnerability assessment tool and acknowledged that lab staff planned to load it on laptops taken to SROs (b)(7)(E) *Id.* at 40. However, he said he did not know that (b)(7)(E) had never been used or that it had cost $40,000. *Id.*

In his OIG testimony, (b)(6),(b)(7)(C) also testified that he was unaware of the undeployed lab equipment. (b)(6),(b)(7)(C) Testimony Tr. at 45. When (b)(6),(b)(7)(C) was asked about the equipment purchased by the lab that had never been used, he said, "It's the first I've heard of it." *Id.* at 52. (b)(6),(b)(7)(C) testified that he had "never been told" that the lab was not using the equipment that it had purchased. *Id.* He also seemed to have no knowledge of the nature of the equipment. *Id.* at 46-48. When asked if he was familiar with (b)(7)(E) he said, "No." *Id.* at 46. He also said that he had "no recollection" of (b)(7)(E) and did not recall (b)(7)(E) *Id.* at 47-48. Similarly, (b)(6),(b)(7)(C) said that he had never heard of (b)(7)(E) and did not know anything about (b)(7)(E) or (b)(7)(E) *Id.* at 50-51.

During testimony, when (b)(6),(b)(7)(C) was shown (b)(6),(b)(7)(C) s 2011 e-mail to him about the undeployed tools (b)(6),(b)(7)(C) stated that he was still "standing by" his testimony that the lab staff always told him that they were deploying the equipment. *Id.* at 54. Although (b)(6),(b)(7)(C) denied knowing the information in the e-mail that had been sent to him, he asserted that the e-mail referred only to items purchased that year (in 2011) that had not yet been implemented. *Id.* at 53-54. However, the items specifically mentioned by (b)(6),(b)(7)(C) in the 2011 e-mail (b)(7)(E) (b)(7)(E) and (b)(7)(E)) had all been purchased prior to 2009. *See* OIT Chart.

F. ARP Lab Staff Purchased Unnecessary Laptops and (b)(7)(E)

In addition to the above-mentioned equipment and software that were purchased but not used, the OIG found that ARP lab staff over the years purchased many more laptops than were needed for the number of staff assigned to the lab.[17] In 2010, the lab spent $26,310 to buy seven (b)(7)(E) laptops and two (b)(7)(E) laptops and $16,643 to buy (b)(7)(E) products, including four (b)(7)(E) laptops. *See* (b)(7)(E) and (b)(7)(E) Laptop Contracting Documents, attached at Exhibit 19; *see* (b)(7)(E) Laptop Contracting Documents, attached at Exhibit 20; *see also* OIT Chart. At the time all those laptops were purchased, the lab had a staff of only four. (b)(6),(b)(7)(C)

[17] The OIG staff was eventually informed by OIT that the ARP lab had 28 laptops.

This document is subject to the provisions of the Privacy Act of 1974, and may require redaction before disclosure to third parties. No redaction has been performed by the Office of Inspector General. Recipients of this report should not disseminate or copy it without the Inspector General's approval.

Testimony Tr. at 162. In addition to the laptops, the ARP lab purchased two [redacted]—one for [redacted] and one for [redacted]—which cost an additional $1,856. *See* [redacted] Contracting Documents, attached at Exhibit 21.

When he was asked why the ARP lab purchased so many laptops for only four people, [redacted] explained that the lab was anticipating hiring "six to eight" new staff members. [redacted] Testimony Tr. at 162. However, the lab staff did not start to grow until late 2011, more than a year after the laptops were purchased. [redacted] Testimony Tr. at 50. [redacted] also testified that one of the [redacted] laptops was given to [redacted] Testimony Tr. at 158. When asked why it was necessary for [redacted] to have a lab laptop if he did not work in the lab, [redacted] said, "I don't want to question my management."[18] *Id.*

[redacted] testified that the [redacted] computers purchased in 2010 were purchased for [redacted] and himself. [redacted] Testimony Tr. at 55. When asked why two people needed so many computers, [redacted] said they wanted "something more reliable" because [redacted] didn't last."[19] *Id.* at 55-56.

[redacted] also admitted that all the [redacted] computers were purchased for [redacted] and himself. [redacted] Testimony Tr. at 163. [redacted] said that he and [redacted] each wanted a 13-inch [redacted] to take on inspections and that they each also got "two and a half pound" [redacted], which he called the "light ones," for training and meetings. *Id.* at 164. When asked if other people at the SEC received [redacted] to take to training, [redacted] said, "No." He then said that [redacted] wanted to get the [redacted] because he wanted "to try it out . . . and learn to use it [a]nd so [redacted] went along with it." *Id.* at 166. [redacted] then acknowledged that he was [redacted] at the time and said, "I shouldn't have approved it. . . . Bad judgment, a mistake. I apologize." *Id.* at 169. [redacted] also said that, in retrospect, they "should have been more frugal."[20] *Id.* at 166.

G. Lab Staff Made False Statements in Paperwork Submitted to Obtain [redacted] Products

The Federal Acquisition Regulation (FAR) sets forth the acquisition process for the purchase of goods and services by the federal government. *See generally* FAR, at https://www.acquisition.gov/far/. Normally under the FAR, government contracts to purchase goods and services are subject to full and open competition. FAR Subparts 6.1–6.2. In some circumstances, however, other than full and open competition is authorized. FAR § 6.302. In

---

[18] [redacted] testified that he used the [redacted] laptop on one inspection and also used it to check his personal e-mail, but that otherwise it sits on his desk "locked up." [redacted] Testimony Tr. at 43.

[19] [redacted] said that the hard drives "went out" on the [redacted] so the [redacted] were needed for their stability. [redacted] Testimony Tr. at 60. However, [redacted] admitted that he could buy a lot of hard drives for the price of an [redacted] laptop. *Id.*

[20] At one point in his testimony, [redacted] said that [redacted] and that as a result the [redacted] was more comfortable for him to carry. [redacted] Testimony Tr. at 164, 166. However, [redacted] admitted that he never made any request for an accommodation under the Americans with Disabilities Act that would have allowed him to get a lighter laptop. [redacted] Testimony Tr. at 166. [redacted] then admitted that [redacted] to his knowledge and that [redacted] purchased the laptop because he wanted it, rather than because [redacted] *Id.* at 167-69.

This document is subject to the provisions of the Privacy Act of 1974, and may require redaction before disclosure to third parties. No redaction has been performed by the Office of Inspector General. Recipients of this report should not disseminate or copy it without the Inspector General's approval.

those situations, the contracting officer must submit a written justification and approval (J&A) to procure the items; the J&A must outline the rationale for other than full and open competition and the reasons for procuring the items. FAR §§ 6.303-1 and 6.303-2. The J&A is then signed by the "technical or requirements personnel," who, in signing, certify that the information in the J&A is "complete and accurate." FAR § 6.303-2(c).

The OIG found that on August 8, 2010, (b)(6),(b)(7)(C) signed the technical and requirements certifications on two J&As that he later admitted in testimony contained false statements. Both J&As, which had a combined value of $18,499, were for (b)(7)(E) products.

1. J&A for (b)(7)(E) Laptops

The first J&A signed by (b)(6),(b)(7)(C) on August 8, 2010, was for the four (b)(7)(E) laptop computers (two (b)(7)(E) 13-inch laptops and two (b)(7)(E) 13-inch laptops) along with (b)(7)(E) desktops, monitors, and associated protection plans and software applications, at a total cost of $16,643.[21] *See* (b)(7)(E) Laptop Contracting Documents. The J&A for that purchase contained the following statement as the reason for obtaining the (b)(7)(E) computer products:

> It is important for the Cyber Security Research Group within the Division's Office of Market Continuity to develop diverse knowledge of common IT operating systems and platforms in use at the Self-Regulatory Organizations . . . . (b)(7)(E) computers are becoming more common in the finance field . . . . It is critical that the Division has industry knowledge of all common computer platforms to carry out this deliverable. The Cyber Security Research Group has seen increased use of (b)(7)(E) computers at SROs.

Id.

When (b)(6),(b)(7)(C) was shown the J&A during his testimony, he admitted that SROs are "not commonly" using (b)(7)(E) and that he had made "an untruthful statement" in the J&A. (b)(6),(b)(7)(C) Testimony Tr. at 171. (b)(6),(b)(7)(C) testified that his certification was "inaccurate," that he "made a mistake," that he does not know why he used that language, and that he "wanted to buy the (b)(7)(E) *Id.* at 173-74. While (b)(6),(b)(7)(C) testified that they were "starting to see" (b)(7)(E) products in "certain exchanges," he could not say which exchanges were using them. *Id.* at 169.

---

[21] After (b)(6),(b)(7)(C) testimony (b)(6),(b)(7)(C) attorney produced another J&A to the OIG that was signed by (b)(6),(b)(7)(C) (b)(7)(E) instead of (b)(6),(b)(7)(C) claiming that the one signed by (b)(6),(b)(7)(C) was a draft that was initially submitted to the contracting office but returned because some changes were necessary. (b)(6),(b)(7)(C) attorney further stated that (b)(6),(b)(7)(C) made the requested changes and signed and submitted the new J&A, which was the actual J&A that was submitted to procure the (b)(7)(E) computers. *See* Alternate (b)(7)(E) J&A, Aug. 19, 2010, attached at Exhibit 22. The OIG confirmed with the SEC's Office of Acquisitions that the J&A signed by (b)(6),(b)(7)(C) that was submitted by (b)(6),(b)(7)(C) attorney was the one used for the procurement. However, the revised J&A contained the same pertinent information as the J&A signed by (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) signed the revised J&A on (b)(6),(b)(7)(C) behalf because (b)(6),(b)(7)(C) was (b)(6),(b)(7)(C)

This document is subject to the provisions of the Privacy Act of 1974, and may require redaction before disclosure to third parties. No redaction has been performed by the Office of Inspector General. Recipients of this report should not disseminate or copy it without the Inspector General's approval.

When [redacted] was asked if any SROs use [redacted] products, he testified that the [redacted] Testimony Tr. at 57. However, [redacted] acknowledged that out of what he estimated to be the approximately [redacted] *Id.* at 58-59.

Other current and former SEC employees confirmed in their OIG testimony that SROs and exchanges do not commonly use [redacted] products. [redacted] Testimony Tr. at 53; [redacted] Testimony Tr. at 30; [redacted] Testimony Tr. at 49; [redacted] Testimony Tr. at 46. Former ARP employee [redacted] testified that [redacted] products are not used at SROs because they are "expensive" and "not very widely supported." [redacted] Testimony Tr. at 53. Former ARP [redacted] also testified that the [redacted] the lab purchased were not needed because "those are not technologies that trading systems are dependent on." [redacted] Testimony Tr. at 30. In addition, SEC [redacted], who previously worked [redacted] told the OIG during testimony that SROs use [redacted][22] [redacted] Testimony Tr. at 49.

The OIG found that [redacted] himself acknowledged in a 2011 e-mail exchange that SROs were not using [redacted] products in their trading operations. In an e-mail dated May 17, 2011, [redacted] wrote to [redacted]

> We don't audit entities that [use [redacted] . . you let me know when you find out that any of the SROs are using [redacted] as one of their standard platforms in their environment or moving towards that direction. Before that I can't support inverting [sic] meaningful time and resources from a group perspective.

E-mail exchange between [redacted] and [redacted] May 17, 2011, attached at Exhibit 23.

[redacted] responded to [redacted] e-mail saying simply, "Smart answer . . . ☺." *Id.* [redacted] explained in testimony that he wrote the e-mail because he was concerned that the lab was purchasing [redacted] when he was "not see[ing] a lot of [redacted] being used" at SROs. [redacted] Testimony Tr. at 46. [redacted] stated in his OIG testimony that he did "not dispute" [redacted] statement that SROs were not using [redacted] which was why he responded to [redacted] e-mail with simply "smart answer" followed by a smiley face. [redacted] Testimony Tr. at 181.

2. J&A for [redacted]

The second J&A that [redacted] signed on August 8, 2010, was for the two [redacted] both with [redacted] and the associated protection plan, for a total of $1,856.[23] *See* [redacted]

---

[22] [redacted] worked at the [redacted] for [redacted] years before coming to the SEC. [redacted] Testimony Tr. at 6.

[23] Again, after [redacted] testimony, [redacted] attorney produced another J&A to the OIG, which was signed by [redacted] and which the OIG confirmed was the one the contracting office used for the procurement of the [redacted] *See* Alternate [redacted] J&A, Aug. 19, 2010, attached at Exhibit 24. This J&A was also substantially similar to

This document is subject to the provisions of the Privacy Act of 1974, and may require redaction before disclosure to third parties. No redaction has been performed by the Office of Inspector General. Recipients of this report should not disseminate or copy it without the Inspector General's approval.

Contracting Documents. The J&A stated that the [redacted] were required because of the need for an "ultra lightweight computer device" to conduct [redacted] *Id.* The J&A further stated that [redacted] is the lightest computer device that offers the functionalities needed" and that "[t]his product is essential in order to simulate trading environments at SROs." *Id.*

When shown the [redacted] J&A, [redacted] immediately acknowledged his signature on the document and said, "[T]his was a very bad judgment call. [redacted] wanted to get the [redacted] I should not have gone along with it. I'm responsible for it, and . . . it was a very bad judgment call . . . ." [redacted] Testimony Tr. at 181. [redacted] said he did not recall who on the staff wrote the [redacted] J&A he signed, but said it could have been [redacted] *Id.* at 184. However, [redacted] admitted that it was "very wrong" of him "to not read [the J&A] in detail" before signing it and that he "should have disagreed with [redacted] because there was "no need for [them] to get the [redacted]" *Id.* at 185.

[redacted] further testified that the J&A he signed for the [redacted] contained a false statement, acknowledging that he could not use an [redacted] for [redacted] because there are [redacted] to hook up the device to do the [redacted] *Id.* at 184. [redacted] said he discussed the [redacted] purchase with both [redacted] and [redacted] but admitted that there is nothing in writing showing that [redacted] and [redacted] approved the [redacted] purchase. *Id.* at 182-83.

In his OIG testimony, [redacted] said that the original intention behind purchasing the [redacted] was to use them for [redacted] Testimony Tr. at 64. However, [redacted] *Id.* at 62-65.

[redacted] confirmed that ARP lab staff were not doing [redacted] when the [redacted] were ordered. [redacted] Testimony Tr. at 62-63. He stated that the lab had not done [redacted] since before he came on board, in October 2009. *Id.* at 63. [redacted] also stated that he did not believe that [redacted] can be done using an [redacted] because an [redacted] does not have [redacted] *Id.* at 64-65.

[redacted] said that he remembered hearing about the [redacted] before they were purchased and that he "guessed" he gave his approval for them "verbally." [redacted] Testimony Tr. at 50. However, [redacted] said he did not know that the justification submitted to procure the [redacted] stated that they would be used for [redacted] *Id.*

In general, [redacted] did not seem to know much about the PRs that were submitted, and in an e-mail dated September, 21, 2010, [redacted] asked [redacted] how many PRs the ARP lab submitted each year. E-mail from [redacted] to [redacted] Sept. 21, 2010, attached at Exhibit 25. [redacted] testified that he had not known that it was "30 or more" until [redacted] gave him this information." [redacted] Testimony Tr. at 57; *see also* E-mail from [redacted] to [redacted] Sept. 21, 2010. [redacted] said he did not know whether the ARP lab had a system to track the PRs it submitted.

---

the one signed by [redacted] Furthermore, testimony confirmed that [redacted] and [redacted] worked together on the J&A and that [redacted] was the responsible [redacted] at the time. [redacted] Testimony Tr. at 181.

This document is subject to the provisions of the Privacy Act of 1974, and may require redaction before disclosure to third parties. No redaction has been performed by the Office of Inspector General. Recipients of this report should not disseminate or copy it without the Inspector General's approval.

[redacted] Testimony Tr. at 57. He admitted that when his staff were gathering PRs for the OIG investigation, they had to go to the "procurement people" because the lab did not keep them.[24] *Id.* at 58.

[redacted] also did not know much about the [redacted] purchase. When he was asked why an [redacted] would be needed for an SRO inspection program, he said, "I don't know what [redacted] are used for in general let alone why they'd be used in an exchange." [redacted] Testimony Tr. at 73. [redacted] further said he had never heard the term [redacted].[25] *Id.* at 74.

II. [redacted] and [redacted] Admitted to Personal Use of SEC Equipment

[redacted] and [redacted] both admitted that they used the [redacted] they purchased mostly for personal purposes. [redacted] Testimony Tr. at 186; [redacted] Testimony Tr. at 61. [redacted] said he used his [redacted] to search the web and to look at his personal e-mail account. [redacted] Testimony Tr. at 61. [redacted] said he used his [redacted] to download computer programming books and otherwise it "has not been put to any substantial use." [redacted] Testimony Tr. at 186. [redacted] also said that he had used his [redacted] to go to iTunes and to download books, such as Tolstoy's *War and Peace*, and magazines. *Id.* at 186-87.

In addition to finding that [redacted] and [redacted] used the [redacted] primarily for personal purposes, the OIG found that they each took home an ARP lab laptop, which they kept at home for personal use. [redacted] testified that he took a [redacted] laptop home with him after using it on a couple of inspections and kept it at his house for "a couple of years," using it primarily for downloading music and movies from iTunes and surfing the web.[26] [redacted] Testimony Tr. at 69-72, 139. [redacted] testified that for nine months or more he kept an [redacted] laptop at his home and used it for personal banking and for checking personal e-mail. [redacted] Testimony Tr. at 192-94. [redacted] also testified that he took the [redacted] laptop with him on vacations to [redacted] *Id.* at 49-50, 187-88.

[redacted] testified that he did not give [redacted] permission to take home a laptop and said he did not know that [redacted] had an ARP lab laptop at his home for two years. [redacted] Testimony Tr. at 48-49. [redacted] also testified that he did not know [redacted] had a laptop at home for two

---

[24] The OIG was unable to obtain the PRs for all the equipment purchased by the ARP lab because the lab did not keep all of them, and OIT could not separate the PRs submitted by the ARP lab from all the other OIT PRs.

[25] In addition to submitting false paperwork for the [redacted] laptops and [redacted] sent an e-mail to [redacted] in October 2009 requesting that his and [redacted] SEC-issued [redacted] be replaced with [redacted] stating, [redacted] and we need to understand the [redacted] security [redacted] *See* E-mail from [redacted] to [redacted] Oct. 23, 2009, attached at Exhibit 26. In testimony, however, [redacted] admitted that his statement to [redacted] about the reason for purchasing the [redacted] was not truthful; he said that he requested an [redacted] because he "wanted to use it" for himself. [redacted] Testimony Tr. at 211. In his reply to [redacted] e-mail, [redacted] stated that [redacted] would need to submit a PR to procure the devices, and [redacted] pointed out that [redacted] had not been approved for use on the SEC network and that [redacted] encryption can be easily cracked. E-mail from [redacted] to [redacted] Oct. 23, 2009. [redacted] testified that he believed that OIT rejected the request for [redacted] as "being excessive." [redacted] Testimony Tr. at 55.

[26] [redacted] testified that he downloaded 200 iTunes onto the laptop. [redacted] Testimony Tr. at 69-70.

This document is subject to the provisions of the Privacy Act of 1974, and may require redaction before disclosure to third parties. No redaction has been performed by the Office of Inspector General. Recipients of this report should not disseminate or copy it without the Inspector General's approval.

years and said he did not give [redacted] permission to take a laptop to [redacted] on vacation.[27] [redacted] Testimony Tr. at 72, 152.

IV. ARP Lab Staff Violated SEC Information Technology Security Policies

The anonymous complaint submitted to the OIG alleged that ARP lab staff, with the knowledge of management, "flagrantly [did] not follow SEC's IT security policies such as Rules of the Road. They use unencrypted security lab laptops during inspections. They have unrestricted access to Internet including being able to check their personal online e-mail services like [redacted] and [redacted]." *See* Anonymous Complaint at 2.

During its investigation, the OIG discovered several areas of concern with regard to computer and network security within the ARP lab. The OIG found multiple instances of recurring violations of SEC policies, which could have caused breaches [redacted] The most egregious violation found was use of unencrypted laptops during inspections, as discussed in detail below.

A. Lab Staff Took Unencrypted Laptops and Laptops Without Virus Protection on Inspections, Potentially Compromising [redacted]

The OIG found during its investigation that lab staff were using laptops that did not have encryption or virus protection during inspections of SROs, exchanges, and clearing agencies [redacted] to those laptops in violation of SEC policy. The OIG further found tha [redacted] as a result.[28]

1. Laptop Computers Purchased by the ARP Lab Were Not Configured by OIT With Security Devices Otherwise Standard on OIT-Issued Computers

The OIG found that the laptops purchased by the ARP lab did not contain the standard security installed by OIT on computers issued to the rest of the SEC staff. SEC [redacted] testified that, to his knowledge, OIT did not do anything to configure or add security to any of the computer equipment purchased by the lab "because it's not standard equipment." [redacted] Testimony Tr. at 42. [redacted] said that for an "agency laptop," OIT "would put [its] image on it and make sure it met [OIT's] security requirements." *Id.* [redacted] believes that equipment ordered by the ARP lab "would just be delivered to them" without any added security. *Id.*

---

[27] [redacted] testified that he was not aware of any documented policies that would prohibit an employee from taking an SEC laptop [redacted] Testimony Tr. at 31. [redacted] also did not think that [redacted] that are of particular concern when laptops [redacted] *Id.* at 32.

[28] The OIG did not examine any files on any ARP lab laptops. Therefore, the OIG does not know other than through witness testimony what [redacted] laptops. As noted later in this report, OIT has contracted with an outside forensics team to conduct forensic testing on selected ARP laptops to determine whether there is evidence that [redacted]

This document is subject to the provisions of the Privacy Act of 1974, and may require redaction before disclosure to third parties. No redaction has been performed by the Office of Inspector General. Recipients of this report should not disseminate or copy it without the Inspector General's approval.

Because the laptops purchased by the ARP lab were not configured by OIT, it was up to their users to install and maintain security devices such as encryption and virus software. (b)(6),(b)(7)(C) Testimony Tr. at 79; (b)(6),(b)(7)(C) Testimony Tr. at 31. As discussed below, the OIG found that several of the lab laptops did not have appropriate security installed but were taken on inspections of SROs, clearing agencies, and exchanges in violation of SEC policy.

SEC OIT policy requires that the local hard drive on all SEC laptop computers be encrypted using approved SAIE software before they are issued to end users. *See* OIT Implementing Instruction 24-04.04.05, Encrypting Data on Portable Media, Dec. 1, 2010, attached at Exhibit 27. This policy also requires that all sensitive, nonpublic, or PII data on portable media, including laptops, be encrypted. *Id.*

SEC OIT policy further prohibits storing nonpublic information or sensitive data on SEC information technology resources "without proper protection/encryption" and "leav[ing] laptop computers containing non-public information or sensitive data unprotected." SEC Rules of the Road, Rule # 7, at 13, attached at Exhibit 28.

2. Several Laptops Identified as Lacking Encryption and Virus Protection Were Used During SRO, Exchange, and Clearing Agency Inspections

On October 17, 2011, the OIG requested from the ARP lab, among other things, documents showing the identity of all lab laptops used off-site during the last year and, for those identified, (1) the date the laptop was last used off-site and the purpose(s) for which it was used; (2) a screen shot showing the name of any antivirus tool used and its version number; and (3) a screen shot showing any encryption tool used and its version number. *See* Document Request, Oct. 17, 2011, attached at Exhibit 29. In response, the lab staff produced the requested information for only 9 of the lab's 28 laptops.[29] *See* Screen Shot Document, attached at Exhibit 30. The screen shots provided of the 9 laptops showed that 4 of the laptops had no antivirus tool installed and 5 had no encryption.[30] *Id.* Of those identified as lacking encryption or antivirus protection, 4 were identified in the Screen Shot Document as having been taken on inspections in the last year. *Id.*

During testimony, the OIG confirmed that the four laptops identified as unprotected and used on inspections were in fact unprotected and used on inspections. The OIG also learned that an additional laptop identified by lab staff as having encryption did not have encryption during the period when it was taken on inspections. Further, the OIG determined that additional laptops—ones that lab staff identified as having protection—may not have had protection until October 2011 and thus would have been taken on inspections unprotected.

---

[29] (b)(6),(b)(7)(C) of OIT informed the OIG that the lab had a total of 28 laptops and that OIT took possession of those laptops when the OIG informed it about the security issues in the lab. It is not currently known how many of those laptops were taken off site or contained SRO, clearing agency, or exchange data. OIT has contracted with an outside agency to perform a forensic evaluation of a selection of those 28 laptops to determine if there was (b)(7)(E) (b)(7)(E)

[30] One of the laptops identified as having no encryption was assigned to (b)(6),(b)(7)(C) an ARP employee who did not work in the lab. This laptop was not identified as having been taken to an SRO so it is not further described below.

This document is subject to the provisions of the Privacy Act of 1974, and may require redaction before disclosure to third parties. No redaction has been performed by the Office of Inspector General. Recipients of this report should not disseminate or copy it without the Inspector General's approval.

The following is a summary of information about the ARP lab's known unprotected laptops, by user.

a. (b)(6),(b)(7)(C)

(b)(6),(b)(7)(C) was identified on the screen shot document as the user of three laptops that lacked security. *See* Screen Shot Document. One was an (b)(7)(E) laptop that had no encryption, but it was identified as having only been taken to (b)(6),(b)(7)(C) by (b)(6),(b)(7)(C) when he was on vacation twice during 2011. *Id.* The other two laptops identified as used by (b)(6),(b)(7)(C) were a (b)(7)(E) that did not have virus protection and an (b)(7)(E) that had neither virus protection nor encryption. *Id.* Both laptops were used on inspections in 2011.[31] *Id.*

(b)(6),(b)(7)(C) testified that the (b)(7)(E) and the (b)(7)(E) were used on inspections, that neither had virus protection, and that the (b)(7)(E) did not have encryption. (b)(6),(b)(7)(C) Testimony Tr. at 174-75; 197-99. (b)(6),(b)(7)(C) called not protecting his laptops "a mistake" and said that he did not have encryption on his (b)(7)(E) "for a really long time." *Id.* at 199. (b)(6),(b)(7)(C) further acknowledged that (b)(7)(E) on his unprotected laptops that (b)(7)(E) (b)(7)(E) and included (b)(7)(E) (b)(7)(E) *Id.* at 199-200. (b)(6),(b)(7)(C) stated that based on his professional education, it was the "dumbest mistake" to (b)(7)(E) computer that had no virus protection. *Id.* at 202.

(b)(6),(b)(7)(C) admitted that the (b)(7)(E) like any computers, are "very (b)(7)(E) and can be compromised," and he agreed that a hacker could hack (b)(7)(E) as easily as a (b)(7)(E) computer. *Id.* at 175-76. (b)(6),(b)(7)(C) further said that he did not have intrusion detection software so he would not know if there was malware on his computer or if it had been hacked. *Id.* at 176-77.

b. (b)(6),(b)(7)(C)

(b)(6),(b)(7)(C) was identified on the screen shot document as the user of two laptops that had encryption but lacked virus protection. *See* Screen Shot Document. One was a 17-inch (b)(7)(E) laptop initially identified as used only for training, and the other was a 13-inch (b)(7)(E) (b)(7)(E) laptop identified as having been (b)(7)(E) *Id.*; (b)(6),(b)(7)(C) Testimony Tr. at 86. (b)(6),(b)(7)(C) said he did not put virus protection on the laptops because it "is hard to find anti-virus" software for Apples. (b)(6),(b)(7)(C) Testimony Tr. at 82. (b)(6),(b)(7)(C) admitted

---

[31] According to the screen shot document, (b)(6),(b)(7)(C) (b)(7)(E) was used on inspections (b)(7)(E) (b)(7)(E) The screen shot document also showed that (b)(6),(b)(7)(C) s (b)(7)(E) was used at the (b)(7)(E) (b)(7)(E) (a cyberdefense exercise). (b)(6),(b)(7)(C) (b)(7)(E) (b)(7)(E) according to the screen shot document, was used at (b)(7)(E) (b)(7)(E) *See* Screen Shot Document.

This document is subject to the provisions of the Privacy Act of 1974, and may require redaction before disclosure to third parties. No redaction has been performed by the Office of Inspector General. Recipients of this report should not disseminate or copy it without the Inspector General's approval.

that he took the 13-inch (b)(7)(E) laptop into exchanges and used it to download SRO data. *Id.* at 83, 86.

The screen shot document indicated that (b)(6),(b)(7)(C)'s (b)(7)(E) used on (b)(7)(E) inspection had encryption. However, when the OIG asked (b)(6),(b)(7)(C) whether the laptop had encryption when it was taken to the inspection, (b)(6),(b)(7)(C) admitted that the encryption was not turned on when he took the laptop on inspections and that he had turned it on to produce the screen shot for the OIG. *Id.* at 87-89.

(b)(6),(b)(7)(C) acknowledged the risk of (b)(7)(E) if his unprotected laptop had been stolen or left in a taxi. *Id.* at 90. He testified that the type of data on his unsecure laptop included (b)(7)(E) *Id.* at 125-26. (b)(6),(b)(7)(C) acknowledged that (b)(7)(E) *Id.*

c. (b)(6),(b)(7)(C)

(b)(6),(b)(7)(C) was identified in the screen shot document as having taken an unencrypted (b)(7)(E) laptop on an inspection in (b)(7)(E) *See* Screen Shot Document. (b)(6),(b)(7)(C) testified that the (b)(7)(E) identified in the screen shot was the laptop he generally used for inspections "because it was lighter." (b)(6),(b)(7)(C) Testimony Tr. at 32. (b)(6),(b)(7)(C) acknowledged that his (b)(7)(E) laptop did not have encryption, saying, "[W]e did not use any encryption tool at the time." *Id.* at 37. When asked if any ARP lab laptops had encryption, (b)(6),(b)(7)(C) said he remembered (b)(6),(b)(7)(C) telling him that (b)(6),(b)(7)(C) (b)(7)(E) came with encryption, but (b)(6),(b)(7)(C) thought that the other lab laptops did not have encryption.[32] (b)(6),(b)(7)(C) Testimony Tr. at 37-38. (b)(6),(b)(7)(C) said that "there was no instruction to use [encryption] at the time" from his management and he did not know it was SEC policy to encrypt all laptops. *Id.*

Although the screen shot document indicated that (b)(6),(b)(7)(C),(b)(7)(E) laptop had antivirus software (b)(6),(b)(7)(C) testified that he was unsure whether it had virus protection prior to October 2011. *Id.* at 35. (b)(6),(b)(7)(C) said he put virus protection on the laptop when he installed Windows 7 after the lab moved to the seventh floor, in October 2011. *Id.* at 33. He said that he contacted OIT to get antivirus software and was told that because the lab was "separate from OIT" he "had to go to the (b)(7)(E)[33] to get the antivirus software. *Id.* (b)(6),(b)(7)(C) said that once he downloaded the antivirus software he "applied them to all the machines." *Id.*

d. (b)(6),(b)(7)(C)

(b)(6),(b)(7)(C) was identified in the screen shot document as the user of an unencrypted (b)(7)(E) laptop. *See* Screen Shot Document. Although the screen shot document indicated that he did not take the laptop off site, (b)(6),(b)(7)(C) testified that he took it to an inspection of the (b)(7)(E) (b)(7)(E) (b)(6),(b)(7)(C) Testimony Tr. at 43, 45. (b)(6),(b)(7)(C) testified that he did not

[32] (b)(6),(b)(7) testified that he put encryption on his laptop; however, he said that he did not consult with any SEC security officials in doing so and was therefore unsure whether he complied with OIT policy or whether the software he put on the laptop was a full version or a cut-down version. (b)(6),(b)(7)(C) Testimony Tr. at 97-98, 107.

[33] (b)(7)(E) is a secured site from which SEC employees can download a home use version of the SEC's (b)(7)(E) (b)(7)(E)

This document is subject to the provisions of the Privacy Act of 1974, and may require redaction before disclosure to third parties. No redaction has been performed by the Office of Inspector General. Recipients of this report should not disseminate or copy it without the Inspector General's approval.

know whether his (b)(7)(E) laptop was encrypted, but he said he did not think that he put (b)(7)(E) (b)(7)(E).[34] *Id.* at 40.

3. ARP Lab Staff Were Recommending (b)(7)(E) While Not Using It Themselves

(b)(6),(b)(7)(C),(b)(7)(E)

(b)(6),(b)(7)(C),(b)(7)(E)

4. According to (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) They Were Unaware of Laptop Security Issues

(b)(6),(b)(7)(C) testified that he was unaware that lab laptops lacked encryption and virus protection. (b)(6),(b)(7)(C) Testimony Tr. at 120-22. He also said the lab had never received any written exceptions with respect to compliance with the security requirements of the OIT Rules of the Road. *Id.* at 120. (b)(6),(b)(7)(C) said that the SROs and exchanges would "be pretty angry" if they knew his staff were bringing unprotected laptops on inspections. *Id.* at 122. (b)(6),(b)(7)(C) acknowledged that (b)(7)(E) (b)(7)(E) laptops (b)(7)(E) *Id.* at 123.

[34] After his testimony, (b)(6),(b)(7)(C) submitted to the OIG a list of inspections to which ARP lab staff may have taken unprotected laptops in the last two years. *See* List of Inspections, attached at Exhibit 31. That list contains more inspections than were initially identified in the screen shot document.

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

[35] In a March 2008 e-mail (b)(6),(b)(7)(C) informed (b)(6),(b)(7)(C) that the (b)(7)(E) had expressed concern about the (b)(7)(E) In the e-mail (b)(6),(b)(7)(C) stated (b)(7)(E) raised concerns about (b)(7)(E) (b)(7)(E) (b)(7)(E) (b)(7)(E) even if encrypted." E-mail from (b)(6),(b)(7)(C) to (b)(6),(b)(7)(C) Mar. 28, 2008, attached at Exhibit 33. (b)(6),(b)(7)(C) further stated, "[T]hese concerns or like concerns seem to be a recurring theme." *Id.*

This document is subject to the provisions of the Privacy Act of 1974, and may require redaction before disclosure to third parties. No redaction has been performed by the Office of Inspector General. Recipients of this report should not disseminate or copy it without the Inspector General's approval.

[redacted] said, "They should not have gone in there without [the laptops] being protected, without having these minimal protections. . . . They should certainly have known better." *Id.* at 125-26.

[redacted] did not recall ever discussing encryption or antivirus protection with his staff. *Id.* at 127. As noted earlier, [redacted] said that [redacted] about whether the [redacted] was protected and that he had told them that it was encrypted. *Id.* at 128. [redacted] said he realizes that there will be "a terrible backlash" when the [redacted] *Id.* at 130.

[redacted] similarly acknowledged that he never told his staff to encrypt their laptops. Testimony Tr. at 88-89. Like [redacted] said that he thinks that [redacted] very upset to find out that [redacted] on unencrypted laptops. *Id.* at 92.

[redacted] further testified that the current plan for the ARP program is to eventually take maps of SRO trading and business platforms and bring them into the lab for testing. *Id.* at 99. He admitted, however, that the lab will "need to tighten things up significantly" first. *Id.*

5. Failure of ARP Lab Staff to Take Security Precautions Could Have Resulted in a [redacted]

Although the OIG is not presently aware of an actual breach [redacted] collected by ARP staff, the OIG found several instances in which the information could have been unknowingly exposed. In particular, the OIG found that SEC staff failed to wipe laptops [redacted] and connected laptops to unsecure wireless networks.

For example, [redacted] admitted that he stored [redacted] on his lab laptop and that he [redacted] so he could "refer to the previous year." Testimony Tr. at 45-46. [redacted] acknowledged that doing so was "not a best practice" and said that it "[a]bsolutely" was a bad practice [redacted] *Id.* at 46, 49. [redacted] said that lab staff generally did not wipe laptops [redacted] and thus were [redacted] *Id.* at 177. [redacted] also said he kept [redacted] on an unencrypted external hard drive in his SEC office. *Id.* at 45.

[redacted] testified that it was "not [their] current practice" to wipe the laptops or reimage them [redacted] Testimony Tr. at 112-13. [redacted] testified that wiping data was "something that was talked about," but that there was "nothing written" and the policy was "still being ironed out." Testimony Tr. at 54. [redacted] likewise testified that the lab did not have a policy to wipe laptops [redacted], saying, "We just didn't do it." Testimony Tr. at 92. In addition, he acknowledged that SROs would not be happy to learn that his staff were carrying [redacted] potentially exposing [redacted] *Id.* at 92-93.

In addition to not wiping laptops [redacted] admitted that he used his unencrypted laptop on public wireless connections in hotel rooms. Testimony Tr. at 53. He said that he and his colleagues also used their laptops on the guest wireless [redacted]

This document is subject to the provisions of the Privacy Act of 1974, and may require redaction before disclosure to third parties. No redaction has been performed by the Office of Inspector General. Recipients of this report should not disseminate or copy it without the Inspector General's approval.

(b)(7)(E) *Id.* at 53-54. (b)(6),(b)(7)(C) further said that while he did not know of a situation in which his laptop was compromised, he would leave it in his hotel room and at the exchanges when he went for meals or took a lunch break. *Id.* at 44.

ARP lab staff also testified that they regularly attended a (b)(7)(E) conference in Las Vegas known as (b)(7)(E) and took lab laptops with them. (b)(6),(b)(7)(C) Testimony Tr. at 49, 154; (b)(6),(b)(7)(C) Testimony Tr. at 105-06, 120; (b)(6),(b)(7)(C) Testimony Tr. at 120. (b)(6),(b)(7)(C) acknowledged that he checked his e-mail from his laptop during (b)(7)(E) [presumably using a publicly accessible wireless connection to do so]. (b)(6),(b)(7)(C) Testimony Tr. at 119-20.

B. ARP Lab Staff Abused the Lab's Unrestricted Internet Access by Going to Prohibited Websites That Could Have Infected Lab Computers (b)(7)(E) (b)(7)(E) With Malware and Viruses

The anonymous complaint submitted to the OIG alleged that ARP lab staff had "unrestricted access to [the] Internet including being able to check their personal online e-mail services like (b)(7)(E)." *See* Anonymous Complaint at 2. During its investigation, the OIG confirmed this allegation, finding that lab staff could access any website while in the lab, and in doing so could have infected lab laptops with malware and viruses (b)(7)(E) (b)(7)(E)

(b)(6),(b)(7)(C) testified that the ARP lab had a (b)(7)(E) connection to the Internet that was completely separate from the SEC network. (b)(6),(b)(7)(C) Testimony Tr. at 27. (b)(6),(b)(7)(C) also testified that lab staff brought lab laptops containing (b)(7)(E) into the lab and hooked them up to the (b)(7)(E) connection. *Id.*

(b)(6),(b)(7)(C) testified that the lab had unfiltered Internet access through the (b)(7)(E) connection, which meant that lab employees could access anything from the lab. *Id.* at 272. (b)(6),(b)(7)(C) also said that the lab had no internal rules related to lab employees' use of the lab's Internet connection. *Id.* He said he had seen in the lab's Intrusion Detection System (IDS) logs that lab staff were using sites like (b)(7)(E) and going to gaming sites while in the lab.[37] *Id.* at 273-74, 278. (b)(6),(b)(7)(C) admitted that visiting such websites could compromise a browser and cause malware to be injected into the computer and that these types of sites are frequent hosts to malware. *Id.* at 275, 278. (b)(6),(b)(7)(C) said that he had accessed (b)(7)(E) from the lab but "tries not to." *Id.* at 273.

While (b)(6),(b)(7)(C) testified that he was not aware of staff accessing any inappropriate websites, he admitted that such activity cannot be prevented under the "current setting." (b)(6),(b)(7)(C) Testimony Tr. at 105. (b)(6),(b)(7)(C) testified that he was not aware of staff accessing inappropriate websites from the lab but said that he did not believe that any sites were blocked. (b)(6),(b)(7)(C) Testimony Tr. at 62-63.

[37] According to (b)(6),(b)(7)(C) an IDS "will alert you if somebody's trying to exploit or come in and attack" your network. (b)(6),(b)(7)(C) Testimony Tr. at 18. As part of its investigation, the OIG asked the lab staff for a copy of the IDS logs to see which Internet sites lab staff were accessing. The lab staff told the OIG that those logs were missing and could not be retrieved.

This document is subject to the provisions of the Privacy Act of 1974, and may require redaction before disclosure to third parties. No redaction has been performed by the Office of Inspector General. Recipients of this report should not disseminate or copy it without the Inspector General's approval.

(b)(6),(b)(7)(C) testified that he did not know that the lab had unrestricted Internet access and said he presumed that the lab had "the same kind of equipment that [the rest of] the SEC has." (b)(6),(b)(7)(C) Testimony Tr. at 130-31. However, SEC (b)(6),(b)(7)(C) did know about the lab's (b)(7)(E) connection and said in his testimony that some blocks and monitoring should be put in place to prevent staff from viewing inappropriate or harmful websites. (b)(6),(b)(7)(C) Testimony Tr. at 16-17, 23.

1. Lab Employees Checked Personal E-mail From the Lab in Violation of SEC OIT Policy

Rule # 2 of the OIT Rules of the Road prohibits the use of any Internet-based e-mail account from SEC computers while at work, at home, or on travel unless such use has been authorized by OIT. *See* Rules of the Road Rule # 2. However, the OIG found that most, if not all, lab employees accessed their personal e-mail accounts from the lab's Internet connection using SEC computers.

(b)(6),(b)(7)(C) testified that he used the lab's Internet connection to check his personal e-mails. (b)(6),(b)(7)(C) Testimony Tr. at 92. (b)(6),(b)(7)(C) said he knew that SEC employees were not allowed to check personal e-mails from SEC equipment because of the potential that viruses could be downloaded and then executed on the system. *Id.* Nevertheless, (b)(6),(b)(7)(C) admitted that he opened attachments in personal e-mails he received from his friends using the ARP lab network and acknowledged that the computer he used to do so (b)(7)(E) *Id.* at 93-94.

(b)(6),(b)(7)(C) testified that he too checked his personal e-mail accounts while in the lab even though he knew it was against SEC policy to do so. (b)(6),(b)(7)(C) Testimony Tr. at 268-69. He testified that other employees also checked personal e-mail from the lab and that when he was monitoring the IDS he could see traffic going to (b)(7)(E) [38] *Id.* at 269.

(b)(6),(b)(7)(C) testified that he checked his personal e-mail accounts from the ARP lab. (b)(6),(b)(7)(C) Testimony Tr. at 99. He testified that he was aware that the rest of the SEC could not access personal e-mail accounts for "security reasons" and said that doing so could "potentially contaminate the computer." *Id.* at 100. (b)(6),(b)(7)(C) further acknowledged that in the case of the ARP lab, an infected computer could be taken on an inspection. *Id.* (b)(6),(b)(7)(C) also said that he would not necessarily know whether a computer he used to access his personal e-mail was infected and that he could not be sure that he never took an infected computer to an inspection. *Id.* at 100-01.

(b)(6),(b)(7)(C) testified that he believed he had seen ARP lab employees checking personal e-mail from the lab and he admitted to doing it himself "on occasion." (b)(6),(b)(7)(C) Testimony Tr. at 62. (b)(6),(b)(7)(C) also acknowledged the risk of infecting the SEC laptop that he takes on SRO inspections with viruses and malware by opening personal e-mails. *Id.*

---

[38] (b)(6),(b)(7)(C) also said that that he used to see on the IDS that lab employees were going to (b)(7)(E) accounts. (b)(6),(b)(7)(C) Testimony Tr. at 34-36.

This document is subject to the provisions of the Privacy Act of 1974, and may require redaction before disclosure to third parties. No redaction has been performed by the Office of Inspector General. Recipients of this report should not disseminate or copy it without the Inspector General's approval.

The OIG found that even some employees who did not work in the ARP lab used the lab computers to check personal e-mail accounts. (b)(6),(b)(7)(C) who worked in the ARP inspection program but not in the lab, testified that he asked for access to the lab to check his personal e-mail account on (b)(6),(b)(7)(C) s computer. (b)(6),(b)(7)(C) Testimony Tr. at 63-64 (b)(6),(b)(7)(C) also said that when he went into the lab he saw that (b)(6),(b)(7)(C) already had his own e-mail account up on the computer screen. (b)(6),(b)(7)(C) Testimony Tr. at 64.

Similarly, (b)(6),(b)(7)(C) admitted to checking his personal e-mail account from his (b)(7)(E) lab laptop in the ARP lab. (b)(6),(b)(7)(C) Testimony Tr. at 43. (b)(6),(b)(7)(C) said he thought he was allowed "incidental use" of SEC equipment but acknowledged that he could not check his personal e-mail from his nonlab SEC computer because he assumed that "OIT blocks that." *Id.* at 44. (b)(6),(b)(7)(C) said he was familiar with the OIT Rules of the Road and took the Rules of the Road training "every year like everyone else," but he said that he did not "explicitly" remember seeing the part about personal e-mail.[39] (b)(6),(b)(7)(C) Testimony Tr. at 44.

2. Lab Staff Downloaded Freeware From the Internet to Unprotected Laptops

(b)(6),(b)(7)(C) testified that one of the reasons he accessed his personal e-mail accounts from the ARP lab was to avoid getting spam in his SEC e-mail box when he signed up for "freeware." (b)(6),(b)(7)(C) Testimony Tr. at 269-70. Although downloading freeware is specifically prohibited under the OIT Rules of the Road (rule # 2 and rule # 9), (b)(6),(b)(7)(C) testified that he downloaded freeware, such as (b)(7)(E) (a free security scanner), to his unprotected lab laptop.[40] (b)(6),(b)(7)(C) Testimony Tr. at 60. He said that he used the freeware to (b)(7)(E) and that the results (b)(7)(E) were stored on his laptops. *Id.* at 57, 61.

(b)(6),(b)(7)(C) acknowledged that freeware he downloaded might have had license restrictions prohibiting its use for commercial or government purposes, but he denied that such restrictions were the reason he used his personal e-mail address to sign up for freeware.[41] (b)(6),(b)(7)(C) Testimony Tr. at 270-71.

(b)(6),(b)(7)(C) said he installed "open source" freeware, such as Notepad++, on his unprotected lab laptop. (b)(6),(b)(7)(C) Testimony Tr. at 85-86. (b)(6),(b)(7)(C) also said that he did not get permission from anyone to install the freeware on his lab laptop and did not check the license agreement to see whether the freeware he downloaded could be used for government purposes, but said he did not use it that often. *Id.* at 86. (b)(6),(b)(7)(C) said that he believed that both (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) used freeware to

---

[39] (b)(6),(b)(7)(C) also acknowledged in testimony that he was aware of the OIT Rules of the Road, took the relevant training, and had not received a waiver or been granted an exception to those rules. (b)(6),(b)(7)(C) Testimony Tr. at 196. (All SEC employees are required to take annual cybersecurity awareness training that includes training on the OIT Rules of the Road.)

[40] Rule # 2 of the OIT Rules of the Road includes the following statement: "DO NOT download or install any software from the Internet. This includes freeware, shareware, public domain software, Web plug-in software such as video players, video streaming software, sound recorders/players, MP3 music files or any instant messaging (IM) software." Rule # 9 of the OIT Rules of the Road includes the following statement: "Do NOT install or use commercial, personally owned, public domain, freeware or shareware software on any SEC computer."

[41] OIT Rules of the Road Rule # 2 also prohibits the downloading of files that violate copyright laws.

This document is subject to the provisions of the Privacy Act of 1974, and may require redaction before disclosure to third parties. No redaction has been performed by the Office of Inspector General. Recipients of this report should not disseminate or copy it without the Inspector General's approval.

(b)(7)(E) . *Id.* at 89-90. Specifically (b)(6),(b)(7)(C) said (b)(7)(E) freeware was used to run a scan of (b)(7)(E) from the lab in March 2012. *Id.* at 89.

3. The Lab's Intrusion Detection and Prevention Systems Were Down for Several Months, Potentially Diminishing Network Security

The ARP lab network is protected by a firewall, an IDS, and (operating in conjunction with the IDS) an Intrusion Protection System (IPS).[42] (b)(6),(b)(7)(C) Testimony Tr. at 27; (b)(6),(b)(7)(C) Testimony Tr. at 18. However, the OIG found that the IDS and the IPS, also referred to by the brand name (b)(7)(E) were not in use for several months, but lab staff continued to use the network.

(b)(6),(b)(7)(C) testified that (b)(7)(E) was "powered . . . out" when the lab was moved to the seventh floor, but he also admitted that the license had expired some time previously. (b)(6),(b)(7)(C) Tr. at 212-13. He estimated that the IDS and IPS were actually down for as long as six months in 2011. (b)(6),(b)(7)(C) Testimony Tr. 214. (b)(6),(b)(7)(C) said that while the IDS and IPS were down, lab staff continued to use the lab's Internet connection. *Id.* at 223-24. (b)(6),(b)(7)(C) said that running the lab with no IDS or IPS was "exposing the lab to major vulnerabilities and compromises . . . ." *Id.* at 224. (b)(6),(b)(7)(C) also said that without the IDS, he would not have been alerted to an intrusion that potentially exposed (b)(7)(E) *Id.* at 225.

(b)(6),(b)(7)(C) testified that ARP lab staff should have severed the lab's Internet connection when the IDS and IPS were not functioning. (b)(6),(b)(7)(C) Testimony Tr. at 19. (b)(6),(b)(7)(C) testified that in a small environment a firewall might be enough protection, but if "it's a larger environment where it's just impossible to keep up with all the firewall logs, you want something more stringent like a (b)(7)(E) or (b)(7)(E) or something like that."[43] *Id.* at 21.

(b)(6),(b)(7)(C) testified that he did not know the IDS and IPS were down until he received the OIG's request for the lab's IDS logs and his staff could not retrieve them. (b)(6),(b)(7)(C) Testimony Tr. at 65. (b)(6),(b)(7)(C) testified that he remembered a "very painful discussion" with his staff about the missing logs. *Id.* at 61. (b)(6),(b)(7)(C) said that (b)(6),(b)(7)(C) was managing the IDS and IPS systems at the time and that (b)(6),(b)(7)(C) frequently had problems with letting licenses lapse. *Id.* at 65-66. (b)(6),(b)(7)(C) said that he did not think the fact that the IDS logs were missing meant that his employees did "anything nefarious with [the lab's] systems."[44] *Id.* at 62.

(b)(6),(b)(7)(C) testified that he could not explain how the IDS logs were lost even though he managed the IDS. (b)(6),(b)(7)(C) Testimony Tr. at 214, 218-219. He testified that he "should have

---

[42] (b)(6),(b)(7)(C) described the function of an IPS as "more of a protective mechanism" with "certain rules and signatures you can put in there for it to block specific types of attacks." (b)(6),(b)(7)(C) Testimony Tr. at 18-19.

[43] (b)(7)(E) and (b)(7)(E) are brand names for IDS and IPS. The ARP lab used (b)(7)(E) as its IDS/IPS system beginning in 2010. (b)(6),(b)(7)(C) Testimony Tr. at 29-30.

[44] Although the IDS logs prior to October 26, 2011, seem to be inexplicably and irretrievably lost, the ARP lab did turn the IDS back on and gave the OIG logs for October 26, 2011, to November 18, 2011. OIG staff reviewed those logs and found that most of the traffic went to (b)(7)(E) and (b)(7)(E) The OIG also attempted to get logs from the laptops themselves but found that the laptops' Internet history logs showed no past websites, likely due to recent reformatting to install (b)(7)(E)

This document is subject to the provisions of the Privacy Act of 1974, and may require redaction before disclosure to third parties. No redaction has been performed by the Office of Inspector General. Recipients of this report should not disseminate or copy it without the Inspector General's approval.

done a better job . . . working with OIT" to make sure that the licenses did not lapse because they "were completely vulnerable." *Id.* at 212.

C. Lab Staff Brought Personal Computers Into the Lab and Connected Them to the Lab Network

During its investigation, the OIG learned of occasions when lab employees connected personal computers to the lab network, resulting in the risk that viruses or other security threats could be introduced into the network and any computer connected to the network. During a visit to the ARP lab in the course of this investigation, an OIG staff member asked about a laptop that was connected to the lab network and was told that the laptop was the personal laptop of a lab employee. When the OIG described this incident during testimony to SEC (b)(6),(b)(7)(C) he said, "I'm not comfortable with anybody conducting . . . Commission business on their own personal machine. We have no idea how it's configured, what weaknesses are in there, what's been patched, not patched, what they're introducing to the environment. I wouldn't—I don't think it's the right thing to do, period." (b)(6),(b)(7)(C) Testimony Tr. at 31.

The OIG also discovered that (b)(6),(b)(7)(C) brought in his personal computers and had his subordinates perform work on them during business hours. The anonymous complaint alleged that (b)(6),(b)(7)(C) gained (b)(6),(b)(7)(C) s favor by performing personal favors for (b)(6),(b)(7)(C), such as fixing (b)(6),(b)(7)(C) personal computer. Anonymous Complaint at 1. When asked about this allegation, (b)(6),(b)(7)(C) testified that he did work on (b)(6),(b)(7)(C) personal computer. (b)(6),(b)(7)(C) Testimony Tr. at 288. However (b)(6),(b)(7)(C) said the computer was "very old" and he "wasn't able to fix it." *Id.*

(b)(6),(b)(7)(C) testified that he also recalled (b)(6),(b)(7)(C) bringing in his personal laptop and asking the lab staff to look at it during business hours. (b)(6),(b)(7)(C) Testimony Tr. at 37. In an e-mail dated January 13, 2011, (b)(6),(b)(7)(C) asked (b)(6),(b)(7) to install (b)(7)(E) and (b)(7)(E) on (b)(6),(b)(7)(C) s personal laptop in the lab. *See* E-mail from (b)(6),(b)(7)(C) to (b)(6),(b)(7)(C) Jan. 13, 2011, attached at Exhibit 34. (b)(6),(b)(7)(C) testified that he remembered installing the software on (b)(6),(b)(7)(C) s personal computer in the lab during business hours and that it took him "maybe 10, 15 minutes." (b)(6),(b)(7)(C) Testimony Tr. at 108-09. (b)(6),(b)(7)(C) said he did not think that (b)(6),(b)(7)(C) paid for the (b)(7)(E) licenses. *Id.* at 116. (b)(6),(b)(7)(C) said he also installed (b)(7)(E) antivirus software on (b)(6),(b)(7)(C) s personal computer and to do so he had to connect (b)(6),(b)(7)(C) s laptop to the lab network to get to the Internet. *Id.* at 110-11. (b)(6),(b)(7)(C) admitted that he did not know what would have stopped (b)(6),(b)(7)(C) s personal computer from infecting the lab network if the computer had had security issues, particularly if the computer had previously lacked virus protection. *Id.* at 111.

While (b)(6),(b)(7)(C) did not know of any specific instances of (b)(6),(b)(7)(C) bringing his personal computers into the lab (b)(6),(b)(7)(C) testified, "The rumor is that (b)(6),(b)(7)(C) [would] bring in his laptop and have somebody in the lab staff help him and get it fixed again, . . . try to get it working again. But I couldn't tell you that that actually happened, and I don't—I've never seen it happen." (b)(6),(b)(7)(C) Testimony Tr. at 94.

(b)(6),(b)(7)(C) told the OIG that he did not have a policy about bringing personal computers into the ARP lab and admitted that he had brought in his old personal laptop three or four years earlier for lab personnel "to work on it and find out about the viruses." (b)(6),(b)(7)(C) Testimony Tr. at

This document is subject to the provisions of the Privacy Act of 1974, and may require redaction before disclosure to third parties. No redaction has been performed by the Office of Inspector General. Recipients of this report should not disseminate or copy it without the Inspector General's approval.

134-35 (b)(6),(b)(7)(C) said he never got the computer back and that they "still have it" as far as he knows. *Id.* at 135. (b)(6),(b)(7)(C) said that he also brought in his "PC" and "gave it to them," and that "[t]hey worked on the viruses" and then "gave it back to [him]." *Id.* at 136. Although (b)(6),(b)(7)(C) admitted to having staff work on his personal computers, he denied knowing anything about (b)(6),(b)(7)(C) installing software on his computer in 2011, stating, "[I]t's not possible." *Id.* at 139. When shown the January 13, 2011, e-mail from (b)(6),(b)(7)(C) to (b)(6),(b)(7)(C) requesting installation of software on (b)(6),(b)(7)(C) s personal laptop, (b)(6),(b)(7)(C) said, "I don't even know what this is referring to." *Id.* at 141.

D. (b)(6),(b)(7)(C) Sent Unencrypted, Nonpublic Data To and From His Personal E-mail Accounts in Violation of OIT Policy and Risking Exposure of the Data

According to the OIT Rules of the Road, "SEC information that must be protected from unauthorized disclosure or access due to its sensitive nature is considered [nonpublic] information." *See* Rules of the Road, Rule # 7. Nonpublic information "is information generated by or in the possession of the SEC that is commercially valuable, market sensitive, proprietary, related to an enforcement or examination matter, subject to privilege, or deemed [nonpublic] by a division director or office head and not otherwise available to the public." *Id.* Prohibited practices concerning nonpublic information include transmitting it through the Internet or via e-mail unless it is encrypted using SEC-approved encryption, and storing or transmitting it on SEC information technology resources without proper protection and encryption. *Id.*

(b)(6),(b)(7)(C),(b)(7)(E)

This document is subject to the provisions of the Privacy Act of 1974, and may require redaction before disclosure to third parties. No redaction has been performed by the Office of Inspector General. Recipients of this report should not disseminate or copy it without the Inspector General's approval.

V. ARP Lab Staff Spent an Excessive Amount on Training Without Proper Oversight

The OIG found that the ARP lab staff's failure to take adequate information technology security precautions was particularly unwarranted given that the OIG also found that the ARP lab spent hundreds of thousands of dollars on training for its staff. The anonymous complaint made the following allegations with respect to training:

> Despite not having any formal training plans or schedule, (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) inappropriately funneled, for training, over $100,000 to the security lab's four staff members including (b)(6),(b)(7)(C) and $40,000 for the rest of the Division this past year. The egregious part is that the security staff spent the money taking classes (sometimes repeatedly) for knowledge that they should already possess, as they passed themselves as IT security experts. Against SEC rules, the security staff (including (b)(6),(b)(7)(C) were not required to and did not file justifications for training nor form SF 182s, which sets out the conditions for training including continuation of service and reimbursement for the cost of training.

Anonymous Complaint at 1.

From the lab's beginning, in 2006, through 2009, training funds for lab staff were allocated through OIT, along with the lab's equipment and software budget, as a line item in the lab's Investment Plan submitted to PRB. *See* Investment Plans. From 2006 through 2009, PRB approved $346,760 in training for the lab's four or five employees. *Id.*; (b)(6),(b)(7)(C) Testimony Tr. at 227. In 2010, the lab staff requested an additional $105,000 in training funds, this time directly from the Office of Human Resources. The rest of Trading and Markets received only approximately $40,000 in training funds for 2010.[45] (b)(6),(b)(7)(C) Testimony Tr. at 235; *see also* Memorandum from (b)(6),(b)(7)(C) to Risinger, Jan. 22, 2010, attached at Exhibit 35.

A. The Lab Staff's Training Schedule Was Excessive and Affected the Inspection Schedule

(b)(6),(b)(7)(C) testified that the line item for training listed in the Investment Plans submitted by the ARP lab to PRB from 2006 through 2009 shows the actual amounts spent on training. (b)(6),(b)(7)(C) Testimony Tr. at 225. He said that only four or five people used all of that training money, which averaged more than $20,000 per person per year.[46] (b)(6),(b)(7)(C) Testimony Tr. at 225-227. (b)(6),(b)(7)(C) said that most classes lasted one week and that each lab staff member would take about 5 or 6 classes per year. *Id.* at 227-28. However, when (b)(6),(b)(7)(C) was shown his own

[45] The OIG could not confirm that the lab actually spent $105,000 on training in 2010. Documents reviewed by the OIG showed that contracts were set up with SANS and Global Knowledge in 2010 for $30,000 and $25,000 respectively. Documents also showed that $7,790 was spent on the (b)(7)(E) conference in 2010.

[46] In an e-mail to a prospective employee, (b)(6),(b)(7)(C) referred to the $20,000 per person per year training allotment for ARP lab employees, stating, "You can spend more than $20K on training each year, just on yourself." E-mail from (b)(6),(b)(7)(C) to (b)(6),(b)(7)(C) Mar. 21, 2008, attached at Exhibit 36. In that same e-mail, (b)(6),(b)(7)(C) also told the prospective employee that he could "[g]et whatever hardware, software, laptop, PDA, Blackberry, etc. you can desire." *Id.*

This document is subject to the provisions of the Privacy Act of 1974, and may require redaction before disclosure to third parties. No redaction has been performed by the Office of Inspector General. Recipients of this report should not disseminate or copy it without the Inspector General's approval.

development plan for 2008, which listed 10 classes, [redacted] admitted to taking 9 out of the 10 classes listed. *Id.* at 250; *see also* [redacted] Individual Development Plan, May 1, 2008–April 30, 2009, attached at Exhibit 37.

[redacted] said that the training the staff received was "necessary" because the staff "didn't have a security background." [redacted] Testimony Tr. at 228. [redacted] said he believed that because of the training the staff received, [redacted] *Id.*

[redacted] also testified that it was "very challenging" to balance all the training the staff was taking with doing inspections. *Id.* at 228. [redacted] further admitted that he took the same training class twice because he "didn't understand it properly" the first time. *Id.* at 245. When asked if he thought that was an effective and appropriate use of taxpayer money, [redacted] replied, "Do I think—no." *Id.* at 245-46.

[redacted] testified that [redacted] decided how much training money to request each year. [redacted] Testimony Tr. at 98. [redacted] explained that a contract would be set up with a vendor and that lab staff would look up what class they wanted to take and then would ask the Branch Chief, either [redacted] or [redacted] for permission to take the class. *Id.* at 98-99. When they received permission, they would send an e-mail to the contact at the vendor to sign up for the class. *Id.* at 99. [redacted] said the staff only needed permission from their Branch Chief to take a class and did not need permission from [redacted] or [redacted] *Id.*

[redacted] acknowledged that in 2008, he spent over $30,000 on training classes for himself. *Id.* at 108-11. When he was asked how many inspections he conducted in 2008, [redacted] testified, "Maybe five or six, maybe, tops," and admitted that some of his training probably did affect his inspection schedule. *Id.* at 110. However, [redacted] said the lab's priority at the time was "to get the lab going and to get the infrastructure moving." *Id.* [redacted] further acknowledged that sometimes all the lab staff would be out on training at the same time and that nobody was staffing the lab at those times. *Id.* at 111-12.

In his testimony, [redacted] explained that the lab would buy contracts with training vendors such as SANS and Global Knowledge and that the staff would then use a "credit voucher" to take classes from those vendors.[47] [redacted] Testimony Tr. at 23. [redacted] testified that he did not think it was necessary to have such a large training budget for the lab. *Id.* at 22. [redacted] said, "[W]ith that amount of money, you can't feasibly go on training, have holidays and vacation and be gone on inspections and do your normal work. I mean there's not enough weeks in the year." *Id.*

[redacted] testified that he did not know exactly how much was spent on training ARP lab staff, but he said that he did not know of any other office at the SEC that had a bigger per person training budget. [redacted] Testimony Tr. at 66-67. In an effort to explain why the lab's training

[47] According to their websites, SANS is a provider of information security training and Global Knowledge provides information technology, business, and enterprise training.

This document is subject to the provisions of the Privacy Act of 1974, and may require redaction before disclosure to third parties. No redaction has been performed by the Office of Inspector General. Recipients of this report should not disseminate or copy it without the Inspector General's approval.

budget was so large, (b)(6),(b)(7)(C) said that in technology, "things don't stand still, the technology changes," so staff continually needed a large training budget to keep up with new technologies. *Id.* at 71. However, (b)(6),(b)(7)(C) also said that sometimes he had difficulty staffing inspections because lab staff were in training. *Id.* at 67.

(b)(6),(b)(7)(C) testified that he did not believe that the ARP lab spent $20,000 to $30,000 per staff member on training each year, although he acknowledged that they were asking for "lots of money" for training. (b)(6),(b)(7)(C) Testimony Tr. at 94-95. With respect to the "enormous training expenses" for security labs, he added, "My personal belief is it's just—it's excessive. . . ." *Id.* at 95. (b)(6),(b)(7)(C) further testified that he did not believe he gave (b)(6),(b)(7)(C) permission to take nine classes in a year and said, "I can't imagine signing off on nine. . . . I must have been drunk at the time." *Id.* at 104. (b)(6),(b)(7)(C) said he thought that two or three classes a year would be reasonable and anything more "would be excessive." *Id.* at 114.

(b)(6),(b)(7)(C) testified that he thought the lab's training budget seemed "extreme," and he described the cost of $25,000 a year per person for SANS training as "outrageous." (b)(6),(b)(7)(C) Testimony Tr. at 63-64. (b)(6),(b)(7)(C) said that it appeared to him as if the training the lab staff received made them well trained for outside employment, but he did not see any specific benefit to the SEC. *Id.* at 95-96.

B. Lab Staff Were Not Required to Submit SF-182 Forms for Vendor Training or to Sign Continued Service Agreements

Paragraph 5.1, Requesting Internal Courses, of SEC Training and Development Policy, issued June 22, 2007, requires employees to obtain permission from their immediate and second-level supervisors before they register for an internal course. *See* Training and Development Policy, at http://insider.sec.gov/policies_procedures/policies/training-policy.pdf. The policy defines internal courses as "[a]ll courses provided directly by the SEC or by organizations under contract to the SEC." *Id.*, Paragraph 1.1, Definitions.

The OIG found that ARP lab staff did not obtain approval from their second-level supervisors prior to registering for classes with SANS and Global Knowledge, which were under contract to the SEC. The OIG also found that lab staff did not regularly document any supervisory approval they received and did not fill out SF-182 forms for vendor training.[48]

(b)(6),(b)(7)(C) testified that lab staff did not fill out SF-182 forms for vendor training and that he had been told that the forms were not needed (b)(6),(b)(7)(C) Testimony Tr. at 239-40. He described the process he used to sign up for a vendor training class as follows: "So I first—obviously, I have to check with (b)(6),(b)(7)(C) for the inspection schedule . . . and then if the inspection schedule permits and (b)(6),(b)(7)(C) approves it, then I will go to the relevant—call the vender, relevant website." *Id.* at 243. (b)(6),(b)(7)(C) said that he would sometimes send (b)(6),(b)(7)(C) an e-mail and sometimes would "go and talk to him" about the training classes he wanted to take. *Id.* at 244.

[48] SF-182, Authorization, Agreement and Certification of Training, is the Office of Personnel Management form for documenting employee training. Lab staff did fill out SF-182 forms for nonvendor training (e.g., for the (b)(7)(E) conference).

This document is subject to the provisions of the Privacy Act of 1974, and may require redaction before disclosure to third parties. No redaction has been performed by the Office of Inspector General. Recipients of this report should not disseminate or copy it without the Inspector General's approval.

But he admitted that there was no formal process for getting supervisory approval to take a class and no documentation of the approval process. *Id.* at 239, 244.

(b)(6),(b)(7)(C) also testified that ARP lab staff did not fill out SF-182 forms for vendor training. (b)(6),(b)(7)(C) Testimony Tr. at 116. (b)(6),(b)(7)(C) further testified that no mechanism was in place to prevent employees from taking classes to pad their resume instead of what was needed to perform their jobs but that "generally the spirit of the group has been to . . . fulfill the lab function." *Id.* at 117. (b)(6),(b)(7)(C) agreed that for ARP lab employees who left the SEC for other jobs, the training they received prior to leaving was "potentially a factor" in getting their new jobs. *Id.*

(b)(6),(b)(7)(C) testified that lab staff did not use SF-182 forms for lab training because he thought that purchasing the vendor vouchers was adequate approval. (b)(6),(b)(7)(C) Testimony Tr. at 24. (b)(6),(b)(7)(C) left the SEC (b)(6),(b)(7)(C) after having taken almost $50,000 worth of training (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) in the ARP program.[49]

(b)(6),(b)(7)(C) a learning officer with SEC University, testified that SF-182 forms are used primarily for tracking and processing funds allocated by SEC University for training. (b)(6),(b)(7)(C) Testimony Tr. at 26. Therefore, if funds for the vendor training came from a source outside of SEC University, an SF-182 form might not be needed to track the funding. *Id.* at 30. However, (b)(6),(b)(7)(C) acknowledged that another function of SF-182 forms is to track supervisory approval for training requested. *Id.* at 26. The second page of SF-182 forms requires the signatures of the requestor's "immediate supervisor" and "second-line supervisor." *See* Form SF-182 at http://www.opm.gov/forms/pdf_fill/SF182.pdf.

The OIG also found that none of the ARP lab staff were required to sign a continued service agreement and therefore could leave the SEC at any time without having to pay back the money spent on their training. According to paragraph 11.0 of the SEC Training and Development Policy, Continued Service Agreement for Training, "the SEC reserves the right to require an employee to sign a continued service agreement prior to attending a course," and provides that employees selected for courses extending more than 60 calendar days or costing more than $5,000" will execute a written continued service agreement before assignment to the course. *See* Training and Development Policy. The executed continued service agreement would require the employee to continue in government service for a period of one year after completion of the training or pay the expenses incurred by the government related to the training. *Id.*[50]

(b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) both testified that they took a SANS class in 2008 that cost $5,039 each and did not sign a continued service agreement prior to attending the course. (b)(6),(b)(7)(C) Testimony Tr. at 107-108; (b)(6),(b)(7)(C) Testimony Tr. at 246-247. (b)(6),(b)(7)(C) confirmed that his staff

[49] The OIG added up the training listed in various documents provided by ARP staff and concluded that (b)(6),(b)(7)(C) received $47,392 worth of training from 2007 to 2010.

[50] An Office of Human Resources representative informed the OIG that the SEC has treated the policy on continued service agreements as being permissive rather than mandatory. The OIG believes that the policy language is ambiguous and suggests that the Office of Human Resources consider revising the policy to clarify that continued service agreements are mandatory for all courses extending more than 60 calendar days or costing more than $5,000.

This document is subject to the provisions of the Privacy Act of 1974, and may require redaction before disclosure to third parties. No redaction has been performed by the Office of Inspector General. Recipients of this report should not disseminate or copy it without the Inspector General's approval.

never filled out continued service agreements for vendor training. (b)(6),(b)(7)(C) Testimony Tr. at 75. (b)(6),(b)(7)(C) testified that he did not know the rules for continued service agreements. (b)(6),(b)(7)(C) Testimony Tr. at 108.

VI. The SEC Has Already Taken Significant Remedial Actions in This Case

Immediately after taking (b)(6),(b)(7)(C)'s testimony on March 19, 2012, the OIG informed (b)(6),(b)(7)(C) that it had learned that SEC staff had taken unencrypted laptops on inspections of SROs, clearing agencies, and exchanges. The OIG also subsequently notified the SEC's Office of General Counsel and SEC Chairman Schapiro's office of this information.

In response, the SEC took several remedial steps to ensure the immediate safety of (b)(7)(E) (b)(7)(E) OIT informed the OIG that it had taken possession of 28 ARP lab laptops and contracted with an outside forensics team to conduct forensic testing on several select laptops to determine if (b)(7)(E) had occurred.[51]

Additionally, several policy changes were implemented within the ARP lab in order to ensure the security of lab equipment. In a memorandum dated May 29, 2012, SEC (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) explained that "all information received (b)(7)(E) (b)(7)(E) information that has been classified by the Division as non-public information and should be protected against both unauthorized and accidental disclosure." *See* Memorandum to Office of Market Continuity Staff from (b)(6),(b)(7)(C) May 29, 2012, attached at Exhibit 38. In the memorandum, (b)(6),(b)(7)(C) directed staff to, among other things, only use laptops with approved security configurations that have been inspected by management before going on site for inspections. *Id.* (b)(6),(b)(7)(C) also mandated that data be wiped from laptops prior to (b)(7)(E) (b)(7)(E)[52] *Id.*[53]

In addition to making the changes to lab policy, on May 18, 2012, the SEC placed (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) on paid, nonduty status pending the OIG's investigation into whether they were improperly using government-furnished equipment and failed to adequately safeguard sensitive information. On July 23, 2012, the SEC's Branch Chief for Personnel Security Operations notified (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) of a tentative determination to revoke their eligibility for access to classified information and/or occupancy of a sensitive position. (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) subsequently resigned (b)(6),(b)(7)(C)

Conclusion

The OIG investigation found that ARP lab staff spent significant budget dollars purchasing computer equipment and software with little oversight or planning and that a significant portion of that equipment and software was unneeded or never used in the inspection

[51] The SEC's Office of Acquisitions informed the OIG that the forensic testing will cost the SEC approximately $340,750.

[52] (b)(6),(b)(7)(C) was detailed to the Division of Trading and Markets to supervise the ARP program. (b)(6),(b)(7)(C) also informed the OIG that he issued a new ARP Inspection Procedural Manual on August 10, 2012, and that he required all ARP staff attend a training session on the manual.

This document is subject to the provisions of the Privacy Act of 1974, and may require redaction before disclosure to third parties. No redaction has been performed by the Office of Inspector General. Recipients of this report should not disseminate or copy it without the Inspector General's approval.

program. The OIG further found that the lab's purchases of (b)(7)(E) equipment were based on misrepresentations by lab staff in contracting documents that (b)(7)(E) was a common operating system used at SROs and that (b)(7)(E) were needed for (b)(7)(E)

The OIG investigation further found that lab staff were taking unencrypted laptops and laptops without virus protection on inspections (b)(7)(E) (b)(7)(E) to those laptops. Although no lab laptop was reported lost or stolen and the OIG is not presently aware of any actual breach (b)(7)(E) (b)(7)(E) the OIG found that the unprotected laptops were left unattended in hotel rooms and in offices outside the SEC, were at times hooked up to public wireless connections, and were taken to (b)(7)(E) conference. In addition, the OIG found that the laptops were taken from (b)(7)(E) (b)(7)(E) without being wiped (b)(7)(E) and were at times connected to the lab's unfiltered, unmonitored (b)(7)(E) Internet connection, which the staff also used to access personal e-mail and download freeware to the unprotected laptops in violation of SEC OIT policy. The OIG also found that lab staff brought their own personal computers to the lab and connected them to the lab network and that a lab employee used his personal e-mail accounts to transfer (b)(7)(E) to and from his SEC e-mail account in violation of SEC OIT policy.

The OIG found that the multiple violations of SEC OIT security policies occurred despite the fact that the SEC spent hundreds of thousands of dollars training ARP lab staff. The OIG found that the ARP lab spent on average $20,000 per staff member per year on training and that lab staff were not required to fill out training forms, such as the SF-182, or sign continued service agreements.

The OIG further found that (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) exercised very little authority or oversight over the lab and did not take appropriate measures to ensure the security of (b)(7)(E) (b)(7)(E) by lab staff.

Recommendations

Accordingly, the OIG is referring this report to the Director of the Division of Trading and Markets; the Deputy Chief of Staff, Office of the Chairman; the Director of the Office of Human Resources; the General Counsel; the Associate General Counsel for Litigation and Administrative Practice; and the Ethics Counsel for consideration of appropriate administrative action with respect to the individuals responsible for the problems and deficiencies identified in this report who remain employed by the SEC.

In addition, the OIG is making the following recommendations:

- OIT should exercise authority over the ARP lab to ensure that lab equipment is properly secured and accounted for, encryption and virus protection are installed on all computers, and the lab Internet connection is properly filtered and monitored.

This document is subject to the provisions of the Privacy Act of 1974, and may require redaction before disclosure to third parties. No redaction has been performed by the Office of Inspector General. Recipients of this report should not disseminate or copy it without the Inspector General's approval.

- The ARP lab's proposed future equipment purchases should be monitored by another SEC office with sufficient knowledge to determine whether the purchases are appropriate for the lab's mission and are cost-effective.

- ARP lab staff should be required to fill out appropriate forms, such as the SF-182 form, before enrolling in any training, including training offered by prepaid vendors, in order to properly document the approval process for each training class taken by lab staff. The OIG further recommends that the SEC clarify its policy on continued service agreements and consider requiring all SEC employees to sign continued service agreements prior to enrolling in training that costs more than $5,000.

We are also providing this report to the OIG Office of Audits for consideration of conducting follow-up audits of the ARP lab and, more broadly, of the purchase of information technology equipment throughout the SEC, to ensure that proper controls are in place to prevent waste and potential data breaches in the future.

A copy of this report is also being provided for informational purposes to Commissioner Elisse B. Walter, Commissioner Luis A. Aguilar, Commissioner Troy A. Paredes and Commissioner Daniel M. Gallagher.

Submitted: (b)(6),(b)(7)(C) Date: 8/30/12

Concur: (b)(6),(b)(7)(C) Date: 8/30/12

Approved: Jon T. Rymer Date: 31 August 2012